Luís Pedro Rodrigues Abreu

Licenciado em Engenharia Informática

Modelo de Gestão de Identidades e Acessos para Pequenas e Médias Empresas

Dissertação para obtenção do Grau de Mestre em

Engenharia Informática

Orientador: Sérgio de Sá, Associate Partner, EY

Co-orientador: Pedro Medeiros, Professor Associado, Faculdade de Ciências e Tecnologia da Universidade Nova de Lisboa

Júri

Presidente: Nuno Manuel Ribeiro Preguiça
Arguentes: Vítor Manuel Alves Duarte
Vogais: Sérgio de Sá

FACULDADE DE CIÊNCIAS E TECNOLOGIA
UNIVERSIDADE NOVA DE LISBOA

Setembro, 2019

Modelo de Gestão de Identidades e Acessos para Pequenas e Médias Empresas

Este documento foi gerado utilizando o processador (pdf)LaTeX, com base no template "novathesis" [1] desenvolvido no Dep. Informática da FCT-NOVA [2].
[1] https://github.com/joaomlourenco/novathesis [2] http://www.di.fct.unl.pt

Resumo

Ao longo dos últimos anos, a temática da gestão de identidades e acessos tem recebido uma elevada importância na estratégia de cibersegurança das organizações, começando a existir uma maior consciencialização dos perigos resultantes de uma arquitetura de gestão de identidades e acessos ineficaz.

A crescente complexidade dos requisitos de conformidade e segurança, tanto ao nível da informação como de sistemas, tem vindo a colocar uma pressão elevada nas empresas, podendo a ocorrência de transgressões ou acessos indevidos ter efeitos reputacionais e financeiros catastróficos.

Mais do que uma iniciativa de tecnologias da informação (TI), a gestão de identidades e de acessos é uma mudança do ponto de vista organizacional como um todo, sendo fundamental garantir o envolvimento da liderança da organização desde a fase inicial do programa.

Contudo, são várias as tentativas de implementação de uma gestão de identidades e acessos eficiente, que acabam por fracassar devido à definição de uma abordagem inicial demasiado agressiva e ambiciosa. Factores como a ausência de investimento organizacional, a resistência à mudança por parte dos intervenientes envolvidos, ou ainda, a falta de interesse e/ou de conhecimento sobre o tema, contribuem para uma reduzida percentagem de sucesso.

Desta forma, a presente dissertação tem como finalidade a elaboração de um modelo para gestão de identidades e acessos que possa ser usado como guia na implementação destes conceitos em pequenas e médias empresas. O modelo definido tem como base a metodologia global da EY, adaptando-a ao contexto nacional.

A implementação do modelo resultante irá permitir a definição de um programa de gestão de identidades e acessos eficiente, concreto e realista, de forma a reduzir os riscos de acessos indevidos a sistemas e aplicações, a aumentar a produtividade dos diversos utilizadores e, ao mesmo tempo, garantir a conformidade com as politicas e procedimentos de controlo de acessos existentes na organização.

Palavras-chave: Identidade, Acesso, Gestão de Identidades e Acessos, Autenticação, Modelo de controlo de acesso, Perfis, Segurança da Informação

Abstract

Throughout the last years, identity and access management has seen an increasing in importance regarding the definition of the strategy of cybersecurity of organizations, by starting to have a higher notion of the dangers that may result from an ineffective identity and access management architecture.

The increasing complexity of compliance and safety requirements, at both the systems and information levels, started to put a higher pressure on companies, since the occurrence of transgressions or improper accesses may affect the reputation of the company and have catastrophic financial consequences.

More than a simple IT initiative, identity and access management is an important shift in the organizational point of view, being fundamental the involvement of the leadership of the organization since the beginning of the program.

However, there are a lot of attempts to implement such system that end up with failure, thanks to an ambitious and agressive approach. Factors like the absence of organizational investment; the resistance to change; or even the lack of interest or knowledge about the subject, contribute to a small percentage of success.

This way, the current dissertation has as a main goal the elaboration of a model for identity and access management that may be used as an implementation guide on small and medium companies . The model will be based on the global methodology developed by EY.

The implementation of the final model will allow the definition of an efficient, concrete and realistic identity and access management program, that may be able to reduce improper application and system accesses ; increase user productivity; and, at the same time, guarantee the compliance with the entity's access politics and procedures.

Keywords: Identity, Access, IAM, Roadmap, Access Model, Roles, Cyber Security

Índice

Lista de Figuras

Capítulo 1

Introdução

1.1 Contexto

Gestão de identidades e acessos é a disciplina responsável por gerir os recursos de uma organização, apresentando-se como um elemento fundamental de qualquer programa de segurança de informação. Esta disciplina gere desde a identidade e formas de autenticação dos indivíduos (sejam eles clientes, colaboradores ou fornecedores), aos privilégios e autorizações de acessos aos vários sistemas e aplicações que constituem o portfólio aplicacional de uma organização. A gestão de identidades e acessos apresenta como principais objetivos: melhorar e garantir a segurança organizacional, controlar os acessos indevidos aos ativos, aumentar a produtividade dos vários intervenientes e assegurar a conformidade para com as politicas e procedimentos de controlo de acessos existentes na organização [4].

O programa de gestão de identidades e de acessos engloba dois conceitos principais, que, embora distintos, só fazem sentido quando relacionados um com o outro [4]. A gestão de identidades envolve todos os processos e tecnologias utilizadas para gerir o ciclo de vida digital das identidades, sejam elas pessoas, sistemas ou serviços.

Por outro lado, a gestão de acessos envolve todos os processos e tecnologias utilizadas para garantir que os utilizadores têm acesso aos recursos adequados para o desempenho das suas funções e que os respetivos privilégios e permissões atribuídas sejam utilizados de forma apropriada e consciencializada.

1.2 Motivação

Hoje em dia, as organizações fornecem vários serviços, suportados por um portfólio abrangente de aplicações e sistemas. Este portfólio aplicacional envolve inúmeros processos,

que são acedidos por múltiplos intervenientes, possuindo, cada um deles, várias funções atribuídas. Por outro lado, estes serviços são suportados por diversas fontes de armazenamento de dados, muitas das vezes compostas por informação sensível ou com um nível elevado de criticidade para o negócio. Uma gestão de identidades e acessos eficaz permite que os vários componentes trabalhem juntos de forma a proporcionar eficiência, segurança e valor comercial às organizações.

Temos assistido a uma mudança rápida de paradigma no que toca ao envolvimento da tecnologia nas organizações. *Cloud*, tecnologias móveis, a adoção de programas *bring your own device (BYOD)* e muitas outras tendências vieram transformar e aumentar o domínio de ameaças de segurança conhecidas até a data [22].

Desta forma, com vista na evolução, as organizações necessitam de reconhecer a gestão de identidades e acessos como uma disciplina que facilita a interação entre o negócio e os respetivos ativos que o suportam. Para continuarem a ser confiáveis, estas necessitam de se tornar eficazes na proteção da privacidade, proporcionar responsabilidades pelas atividades realizadas e controlar os seus ativos sem sobrecarregar excessivamente a experiência do utilizador.

1.3 Problema

Apesar dos inúmeros benefícios proporcionados por uma eficaz gestão de identidades e acessos, muitas implementações destas soluções acabam por não conseguir atingir os resultados pretendidos ou até mesmo por fracassar [11]. As razões que levam ao seu fracasso são fáceis de identificar mas difíceis de ultrapassar. Fatores como a ausência de investimento organizacional, a resistência à mudança por parte dos intervenientes, ou ainda, a falta de interesse e/ou de conhecimento sobre o tema, contribuem para uma reduzida percentagem de sucesso [4].

As organizações precisam de definir, de forma clara, os objetivos e resultados esperados no processo de transformação digital a que se propõem. 84% das organizações falham neste processo, devido à falta de consciencialização sobre os desafios a enfrentar [15]. O principal objetivo do programa não deve estar relacionado com questões de conformidade para com regulamentos ou políticas. O planeamento passa por compreender as vantagens destas soluções e por definir uma estratégia clara de gestão.

Apesar de existirem *frameworks* de gestão de identidades e acessos bem definidas, como é o caso da *framework* global proposta pela EY [4], estas são, no geral, complexas e, por vezes, demasiado ambiciosas na abordagem que proporcionam, principalmente quando aplicadas a pequenas e médias empresas. Por norma, estas organizações não se regem pelos mesmos objetivos e possuem um conhecimento menos abrangente sobre o tema, tanto a nível dos desafios e problemas que uma fraca gestão de identidade e acessos pode apresentar, como dos vários benefícios que uma implementação eficaz do programa pode proporcionar.

1.4 Objetivos e contribuições

Num cenário em que temas relacionados com a cibersegurança estão na agenda de todas as empresas, a gestão de identidades e de acessos é mais importante do que nunca, de forma a assegurar que cada utilizador tem acesso aos recursos certos, com base em processos eficientes, flexíveis e com risco mitigado.

Para isso, tendo como base *drivers* de negócio, como o aumento da transparência, a redução do risco, o aumento da produtividade e a melhoria da experiência do utilizador, à empresa X, média empresa a operar no setor dos transportes em território nacional, pretende efetuar uma avaliação do seu estado atual no que diz respeito à gestão de identidades e e acessos, tendo como base a *framework* global de maturidade da EY.

Dependendo do nível de maturidade encontrado, serão definidas recomendações e iniciativas de forma a alcançar os resultados pretendidos.

O projeto piloto de gestão de identidades e acessos a realizar na empresa X, proposto pela EY, prevê a concretização dos seguintes passos:

- Identificação e análise do portfólio aplicacional da organização;
- Levantamento de ferramentas de suporte à gestão de identidades e acessos existentes;
- Identificação de soluções tipo para cada *cluster* encontrado;
- Levantamento dos mecanismos de autenticação existentes;
- Análise do modelo de governo existente e definição do modelo futuro;
- Revisão de contas adormecidas e utilizadores privilegiados;
- Identificação de requisitos técnicos e funcionais;
- Analise de *gap* entre o estado atual da organização e o modelo futuro.

Durante a concretização do projeto, pretende-se efetuar uma avaliação crítica à abordagem utilizada, de forma a analisar todos os passos efetuados e descrever um conjunto de etapas e procedimentos cruciais para o seu sucesso.

A presente dissertação apresenta como principal objetivo, a definição e documentação de uma metodologia padrão, simples e pragmática, que serva de base ao planeamento e implementação de novos projetos no âmbito da gestão de identidades e acessos, em contexto nacional. A definição da metodologia e do modelo de gestão de identidades e acessos associado terá como base toda a experiência e conhecimento adquirido durante a realização do referido projeto.

1.5 Estrutura do documento

O restante documento encontra-se estruturado da seguinte forma:

Capítulo 2 (Conceitos e Estado da Arte) Neste capítulo são apresentados os conceitos e conhecimentos adquiridos fundamentais para definição do modelo de gestão de identidades e acessos.

Capítulo 3 (Trabalho relacionado) Neste capítulo é apresentada a visão global da EY e respetiva *framework*, utilizada em projetos de gestão de identidades e acessos.

Capítulo 4 (Análise realizada) Neste capítulo são apresentados os resultados obtidos referentes à análise efetuada à *framework* apresentada no capítulo 3. Posteriormente, é sugerida a metodologia a ser utilizada em projetos futuros.

Capítulo 5 (Fase 1 - Diagnóstico) Este capítulo descreve os passos que constituem a primeira fase da metodologia sugerida. São apresentados também, como exemplo prático, os resultados da análise de maturidade efetuada à empresa X.

Capítulo 6 (Fase 2 - Definição do modelo a aplicar) Neste capítulo é apresentado o modelo de gestão de identidades e acessos definido. São apresentadas recomendações para a definição do modelo de governo, normas e processos.

Capítulo 7 (Fase 3 - Definição do *roadmap* de implementação) Neste capítulo são definidas e descritas as iniciativas de apoio à implementação do modelo definido no capítulo 6.

Capítulo 8 (Validação do modelo) Neste capítulo é efetuada a implementação teórica do modelo definido, seguida de uma análise de maturidade ao estado alcançado. Como exemplo prático, é realizada a implementação do modelo na empresa X.

Capítulo 9 (Conclusão) Conclusão da presente dissertação e discussão sobre o trabalho futuro.

Capítulo 2

Conceitos e Estado da Arte

No presente capítulo são apresentados todos os conceitos e conhecimento adquiridos, fundamentais tanto para elaboração da presente dissertação, como para a realização do projeto em que esta se insere.

O estudo realizado será indispensável na realização dos vários passos que constituem o programa de gestão de identidades e acessos, desde a análise ao portfólio e avaliação de maturidade do estado atual da organização, à definição do modelo de governo futuro a implementar.

De forma a executar os passos referidos, torna-se indispensável adquirir conhecimentos sobre as várias fases do ciclo de vida das identidades, os diferentes mecanismos, protocolos e fatores de autenticação existentes, a noção de perfis de acesso e respetivas permissões e privilégios e possuir uma forte base de conhecimento sobre políticas, normas e processos.

2.1 Princípios fundamentais da segurança de informação

Os conceitos e princípios de gestão de segurança da informação são elementos fundamentais para a definição de politicas de segurança e para a implementação de soluções. Estes definem as metas e objetivos que, tanto os *designers* de políticas, como os implementadores de sistemas, devem alcançar de forma a apresentar uma solução segura.

2.1.1 Tríade CIA

A tríade *CIA* é um princípio fundamental da segurança da informação. Esta ferramenta deve ser conhecida e aplicada por todos os profissionais de segurança da informação de forma a proteger os ativos de uma organização contra acessos indevidos. Este princípio é constituído por 3 conceitos-chave: confidencialidade, integridade e disponibilidade [1].

- **Confidencialidade**: princípio responsável por apresentar medidas de segurança que garantam a proteção e privacidade dos dados, objetos e recursos. Este princípio tem como objetivo providenciar meios para que utilizadores autorizados consigam aceder e interagir com os recursos pretendidos e, ao mesmo tempo, vedar esses mesmos acessos aos restantes utilizadores não autorizados. Um vasto leque de controlos de segurança é usado para providenciar a confidencialidade dos dados, como o recurso a criptografia, controlos de acessos e esteganografia.

- **Integridade**: princípio responsável por manter a confiabilidade e exatidão dos dados de uma organização. Para que um mecanismo de segurança consiga oferecer integridade, este tem de garantir que os dados, objetos e recursos permaneçam inalterados desde o seu estado inicial de proteção. Seja qual for o estado dos ativos (em armazenamento, em trânsito ou em processamento), estes devem apenas ser alterados por utilizadores autorizados. Mecanismos rigorosos de autenticação, sistemas de deteção de intrusões, cifra e *hash* de dados são alguns mecanismos de segurança implementados com vista a manter a integridade.

- **Disponibilidade**: princípio responsável por garantir que os recursos estejam disponíveis sempre que for necessária a sua utilização. Para que um sistema se mantenha disponível, vários controlos de segurança devem ser implementados de forma a proporcionar acesso contínuo aos recursos e a prevenir ataques de negação de serviço (DoS). Este controlos passam por mecanismos de redundância e *back-ups* de forma a prevenir a perda ou destruição dos dados.

  Não-repudiação: assegura que o responsável por uma ação não pode negar a ocorrência de um evento pelo qual foi responsável. A não-repudiação pode ser atingida através de certificados digitais, identificadores de sessão, *logs* de transação e muitos outros mecanismos de controlo de acessos.

2.2 Normas e Frameworks de controlos de segurança

No planeamento de segurança da informação é fundamental adotar uma *framework* ou norma de controlos de segurança de forma a definir uma solução que possa ser aplicada a toda a organização. Existem algumas opções de escolha nesta área:

- COBIT [10]: *framework* com foco empresarial. Apresenta boas práticas para a definição de modelo de governo e gestão da infraestrutura de sistemas, redes e dispositivos que constituem a organização. O COBIT é, maioritariamente, utilizado para definir requisitos de auditoria e conformidade na área de TI.

- ITIL [9]: apresenta um conjunto de boas práticas recomendadas para a gestão de serviços de TI. Este guia promove uma gestão mais focada no cliente e na qualidade dos serviços internos de TI.

- ISO:27002 [19]: norma de boas práticas de suporte à implementação de sistemas de gestão de segurança da informação.

Estas *frameworks* ou normas internacionais proporcionam uma série de controlos de segurança, que podem ser representados através de políticas, normas, processos e procedimentos.

2.2.1 Políticas, normas e processos

A **política** de segurança da informação especifica os objetivos de controlo e deve ser vista como um quadro legislativo. Os objetivos de controlo aplicam-se independentemente da localização e das tecnologias envolvidas. A política de segurança da informação estende-se a toda a organização e parceiros ou fornecedores externos que possuam uma relação institucional ou contratual.

As **normas** são documentos que derivam das políticas e fornecem controlos e diretivas obrigatórias. Deverão ser vistas como um reforço das regras definidas na política global de segurança da informação, fornecendo maior um detalhe e contexto específico.

Os **processos** descrevem um conjunto ordenado de atividades definidas de forma a alcançar o objetivo pretendido.

Os **procedimentos** descrevem sequências de ações e operações que permitem a realização das tarefas de acordo com a política de segurança da informação.

Por fim, existem ainda as **normas técnicas**, documentos que descrevem controlos técnicos, específicos e detalhados. Estes são documentos de natureza técnica e focam-se numa tecnologia específica.

2.3 Identidades e Autenticação

2.3.1 Diferença entre identificação e autenticação

Identificação é o processo em que um sujeito alega a sua identidade. Para que os processos de autenticação, autorização ou responsabilização de um sistema iniciem, é necessário que o sujeito se identifique *à priori*. Esta identificação pode ser fornecida através de um nome de utilizador, um cartão de acesso, um *token*, uma análise de impressão digital ou de muitas outras formas que envolvam algo que o sujeito conheça, seja ou possua [1].

O processo de **autenticação** verifica a identidade do sujeito, comparando um ou mais fatores (*passwords*, *tokens*, etc) com a identidade válida armazenada numa fonte de informação. Para que este processo seja exequível, é fundamental que cada identidade esteja associada a apenas um sujeito e que a informação necessária para realizar a autenticação esteja protegida, recorrendo a método de *hash* ou cifra [1].

2.3.2 Ciclo de vida das identidades

O ciclo de vida das identidades refere-se aos eventos de criação, gestão e remoção de contas de utilizadores. Sem uma gestão clara das identidades, os mecanismos de autenticação, autorização e responsabilização de um sistema serão comprometidos. O ciclo referido é constituído por três conceitos principais [4]:

- **Aprovisionamento de conta**: criação de novas contas de utilizadores. O processo de criação de contas é designado por registo. Neste processo é criada uma nova identidade e definido de que modo esta será comprovada (autenticada) perante os sistemas. É fundamental a definição de regras para criação, de forma a que as contas geradas sejam sempre distintas.

- **Revisão**: as contas de utilizadores devem ser revistas para garantir que estão em conformidade com as políticas de segurança e respetivos processos. Esta revisão deve ter em conta se existem sujeitos com privilégios excessivos para a realização das suas funções.

- **Desativação** e **remoção**: as contas de utilizadores devem ser desativadas e/ou removidas em caso de saída da organização, seja ela temporária ou permanente. Estes casos devem ser notificados pelos recursos humanos, devido à visibilidade que apresentam.

2.3.3 Mecanismos e protocolos de autenticação

- ***Single Sign-On***: técnica de controlo de acessos centralizada que permite a um utilizador autenticar-se apenas uma vez num sistema e ter acessos a múltiplos recursos sem a necessidade de efetuar novamente a autenticação [1].

- **Federação**: utilizando federação, a aplicação não precisa de obter ou armazenar credenciais de utilizadores para realizar a autenticação dos mesmos. Esta pode ser realizada com recurso a um sistema de gestão de identidades, interno ou externo, bastando para isso que a aplicação confie no sistema em questão [18]. Múltiplas organizações podem formar um grupo ou federação, de forma a partilhar identidades entre elas.

- ***Kerberos*** [20]: sistema de *tickets* que utiliza uma entidade *third-party* para comprovar identidades e proporcionar mecanismos de autenticação. *Kerberos* utiliza criptografia baseada em chaves simétricas utilizando o protocolo *AES* (*Advanced Encryption Standard*) para realizar a autenticação entre clientes e servidores. Desta forma, o protocolo providencia confidencialidade e integridade durante o processo de autenticação, protegendo o processo contra ataques de *eavesdropping* e de reprodução [1]. *Kerberos* fornece capacidades de *Single Sign-On* através da criação e partilha de *tickets* de autenticação.

- ***LDAP*** *(Lightweight Directory Access Protocol)*: protocolo que serve de base a vários serviços de diretoria (ex: *Active Directory* [12]). Através deste protocolo de pesquisa, utilizadores e processos obtêm acesso ao sistema pretendido, tendo apenas de se autenticar perante o serviço de diretoria existente na organização. Os acessos são fornecidos de acordo com os privilégios atribuídos à identidade que se autentica.

- ***SAML*** (*Security Assertion Markup Language*): linguagem baseada em *XML* usada para troca de informação de autenticação e autorização entre organizações federadas. *SAML* pode ser usado para proporcionar *Single Sign-on* em acessos via *browser* [1].

- **OAuth2.0** [21]: *open standard* usado para delegação de autorizações. Várias aplicações móveis utilizam este protocolo para pedir autorizações de acesso à informação presente em *websites*, como, por exemplo, *Facebook* ou *Twitter*. Desta forma, o utilizador não necessita de fornecer à aplicação as suas credenciais de acesso ao site.

- **OpenID**: *open standard* que permite que um utilizador se autentique perante uma aplicação ou sistema utilizando um serviço de *third-party* de identidades. O utilizador pode escolher o fornecedor que pretende entre um leque de opções. *Facebook*, *Google* e *Microsoft* são alguns desses exemplos [18].

2.3.4 Fatores de autenticação

Um fator de autenticação é uma categoria de credenciais que tem como objetivo verificar, por vezes em combinação com outros fatores, a identidade de um sujeito. Existem cinco grandes grupos de fatores de autenticação[3]:

- **Algo que conhecemo**s: uma informação é classificada como algo que conhecemos ou sabemos quando se encontra armazenada na nossa memória, podendo ser acedida quando necessitamos. Podemos incluir nesta categoria mecanismos de autenticação como *PINs* ou *passwords*. Nomes de utilizadores ou endereços de *e-mail* não se incluem nesta categoria, dado que apenas têm como propósito alegar uma identidade e não comprová-la.

- **Algo que possuímos**: uma informação é classificada como algo que possuímos quando pode ser mantida fisicamente em nossa posse. O mecanismo de autenticação mais conhecido desta categoria é o *token*. *Tokens* são dispositivos físicos capazes de gerar *one-time passwords*. Estas podem ser geradas de tempo a tempo, por exemplo, 30 segundos, ou mantidas até que o utilizador as utilize (apenas uma vez).

- **Algo que somos**: toda a informação que provém de atributos físicos diferenciadores de um indivíduo, como por exemplo, impressões digitais, retina, íris, voz ou cara.

- **Algo que fazemos**: este tipo de autenticação baseia-se na observação de ações realizadas pelo indivíduo, como por exemplo, gestos ou toques. Um dos exemplos

deste tipo de autenticação é a *Picture Password*, que permite autenticar um utilizador através de cliques numa imagem à sua escolha. O sistema guarda os cliques pré-definidos pelo utilizador e compara-os com os efetuados no momento da autenticação.

- **Algum lugar onde estejamos**: este tipo de informação encontra-se relacionada com a localização de um indivíduo. Este tipo de autenticação recorre a endereços de *IP* ou endereços *MAC* para garantir o acesso pretendido. Por exemplo, sistemas que possuam mecanismos de segurança baseados em geo-localização podem negar o acesso a dispositivos que se encontrem a tentar realizar um pedido de autenticação num local ou dispositivo diferentes dos estipulados pelo utilizador.

O tipo de autenticação pode também ser classificado pela quantidade de fatores utilizados durante o processo, podendo classificar-se em [3]:

- **Autenticação *single-factor***: quando o processo de autenticação é efetuado com recurso a um único fator.

- **Autenticação *two-factor***: quando o processo de autenticação é efetuado recorrendo a dois fatores.

- **Autenticação *multi-factor***: quando são utilizados dois ou mais fatores no processo de autenticação. Este conceito implica a validação de todos os fatores utilizados em simultâneo, enquanto que o mecanismo de autenticação *multi-step* permite que os fatores sejam autenticados de forma sequencial. Este tipo de autenticação não é tão seguro uma vez que permite identificar quais os fatores que levaram ao fracasso do processo de autenticação.

2.4 Acessos e Autorizações

2.4.1 Permissões, direitos e privilégios

O termo **permissões** refere-se às ações que um sujeito pode realizar dentro de um objeto (aplicação ou base de dados). São exemplo de permissões: *create*, *read*, *edit* e *delete* [1].

O termo **direitos** aplica-se, por norma, ao direito de ações sobre sistemas. Como por exemplo, alterar a data e hora de um computador ou poder realizar um *backup*. O termo permissões também pode abranger estes casos [1].

O termo **privilégios** refere-se ao conjunto de permissões e direitos que um utilizador possui [1].

2.4.2 Princípios e mecanismos de autorização

- ***Implicit Deny***: princípio básico de controlo de acessos utilizado por muitos mecanismos de autorização. Este princípio assegura que qualquer acesso a uma determinada aplicação ou sistema é negado a não ser que seja explicitamente atribuído [1].
- ***Need to Know***: princípio que garante que cada utilizador apenas tem acesso ao que necessita de saber para desempenhar as suas tarefas e funções [17].
- ***Least privilege***: princípio que garante que cada utilizador possui apenas os privilégios necessários para desempenhar as suas tarefas ou funções [1].
- **Segregação de funções**: princípio que garante que ações e funções sensíveis ao negócio sejam divididas em tarefas realizadas por dois ou mais colaboradores. Nenhum utilizador deve possuir conjuntos de privilégios que levem ao uso incorreto ou malicioso do sistema alvo [17].
- **Matriz de controlo de acessos**: tabela que inclui utilizadores, aplicações e os respetivos privilégios atribuídos. Esta tabela é acedida pela aplicação ou sistema, para verificar se um determinado utilizador possui os privilégios necessários para realizar a ação pretendida.
- **Interface controlada**: mecanismo de controlo de acessos com base em menus e interfaces. Utilizadores com acesso total podem realizar todas as ações e ter acesso a toda a informação do objeto. Utilizadores normais podem não ter acessos a alguns menus ou controlos, ou estes podem aparecer no ecrã em modo inativado.
- **Controlo baseado no conteúdo**: os acessos são geridos com base na sensibilidade da informação [8]. No caso de uma base de dados, por exemplo, um utilizador pode ter acesso apenas a algumas tabelas ou apenas alguns atributos pertencentes à tabela geral.
- **Controlo baseado no contexto**: os acessos são geridos com base no estado da atividade [8]. Um acesso pode ser negado caso o utilizador não tenha realizado uma atividade *à priori*.

2.4.3 Modelos de controlo de acessos

- **DAC** (*Discretionary Access Control*): modelo de controlo de acessos onde as permissões são atribuídas ao nível do objeto (sistema, aplicação, base de dados) [14]. As permissões são atribuídas pelo responsável pelo ativo pretendido ou por um administrador central.
- **MAC** (*Mandatory Access Control*): modelo de controlo de acessos baseado na classificação dos ativos [1]. Um utilizador só pode ter acesso à informação ou aplicações com uma determinada classificação. Esta classificação pode, por vezes, ser realizada

com base numa estrutura hierárquica, como é o caso das classificações de informação confidencial, secreta e sensível. Um utilizador com acesso à informação no topo da hierarquia (confidencial) pode aceder à informação de todos os tipos de classificação.

- **RBAC** (*Role Based Access Control*): modelo de controlo de acessos baseado em *roles*. Os utilizadores são associados a *roles* e estas estão associadas a um conjunto de permissões [16]. As *roles* são definidas tendo por base as funções de negócio existentes numa organização e são atribuídas a utilizadores tendo em conta as suas qualificações e responsabilidades.

- **ABAC** (*Attribute Based Access Control*): modelo de controlo de acessos baseado em atributos de utilizadores e sistemas. Este modelo foi desenvolvido com vista a diminuir a quantidade de esforço requirido para a definição de *roles*. Ao utilizar atributos, como a hora do dia ou o departamento a que pertence um determinado utilizador, e a classificação de ativos, o modelo *ABAC* fornece mais opções de atribuição de acesso. Esta vasta lista de opções pode levar a um processo tedioso de revisão de acessos [2], devido ao elevado nível de granularidade existente.

2.5 Gestão de Identidades e Acessos - Abordagens

2.5.1 Autenticação e autorizações ao nível da aplicação

Esta abordagem é bastante comum nas organizações, particularmente em aplicações alinhadas com um processo específico de negócio. Neste exemplo, a autenticação é realizada diretamente na aplicação: o utilizador insere as suas credenciais e a aplicação compara os dados introduzidos com os dados armazenados no seu repositório específico.

Apesar de apresentar uma estrutura simplificada, esta abordagem levanta vários problemas se for usada como padrão em toda a organização:

- O utilizador necessita de credenciais específicas para cada aplicação;

- Devido à quantidade de *passwords* existentes (uma para cada aplicação), os utilizadores podem cair no erro de as armazenar fisicamente, originando falhas graves de segurança;

- Torna-se extremamente difícil coordenar o aprovisionamento de acessos e atribuições de *roles*, impossibilitando uma visão holística dos acessos que cada utilizador possui.

2.5.2 Autenticação e autorizações centralizadas

Nesta abordagem, os mecanismos de autenticação e definição de autorizações encontram-se centralizadas, fora do contexto aplicacional. Este método, quando implementado em

uma só aplicação, torna-se mais complexo; mas, quando aplicado a um conjunto maior, apresenta vantagens significativas:

- Proporciona uma visão holística das identidades da organização;
- Atribui um identificador global a cada utilizador, o que facilita a revisão dos acessos atribuídos e;
- Os utilizadores deixam de precisar de um par de credenciais para cada aplicação.

As aplicações integradas nesta abordagem deixam de precisar de armazenar identidades ou de implementar lógica para o controlo de acessos. Todas as identidades encontram-se armazenadas no diretório central. Isto só é exequível em aplicações que apresentem regras de controlo de acessos simples, baseadas em atributos ou grupos de utilizadores.

Desta forma, a aplicação não precisa de alocar tantos recursos, visto que o acesso do utilizador é confirmado ou negado antes da aplicação ser executada. Por outro lado, a definição do mapeamento entre conjuntos de acessos a aplicações e as *roles* existentes na organização pode dar origem a um processo bastante complexo e demorado.

Para as aplicações com privilégios de acesso específicos ou proprietários, continua a ser necessário manter alguma dessa lógica ao nível da aplicação.

Combinando esta abordagem com uma ferramenta de gestão de identidades e acessos, passa a ser possível efetuar de forma automática todos os processos de pedido, aprovação e aprovisionamento de acessos.

Capítulo 3

Trabalho relacionado

Neste capítulo é apresentada a visão global da EY e respetiva *framework*, utilizada em projetos de gestão de identidades. Esta é utilizada por profissionais de cibersegurança, como *guideline* na avaliação do estado de maturidade das organizações.

3.1 *Framework* de Gestão de Identidades e Acessos - EY

De forma a facilitar o entendimento de todos os conceitos envolvidos numa gestão de identidades e acessos eficaz, a EY divide este complexo domínio em dois grupos distintos: gestão de identidades e gestão de acessos.

Gestão de Identidades A gestão de identidades refere-se a todas as pessoas, processos e tecnologias necessárias para gerir o ciclo de vida de identidades. Esta gestão incluiu os seguintes procedimentos:

- Estabelecer identidades únicas e associá-las a credenciais de autenticação;
- Incorporar estas identidades em aplicações, sistemas e plataformas alvo;
- Criar novas contas de utilizadores;
- Gerir a informação referente a identidades;
- Criar fluxos processuais de aprovação para criação de contas;
- Providenciar a capacidade de modificar, suspender ou remover contas;
- Auditar e reportar informação sobre identidades de utilizadores.

Gestão de acessos A gestão de acessos refere-se a todos os processos e tecnologias utilizadas para controlar os acessos atribuídos a uma dada identidade. Esta gestão inclui os seguintes procedimentos:

- Definir métodos de solicitação de privilégios de acessos;
- Implementar fluxos processuais para aprovar a atribuição de privilégios e/ou *roles* a uma identidade;
- Providenciar a capacidade de modificar ou remover privilégios e/ou *roles* associadas a um utilizador;
- Gerir a associação de privilégios e *roles* a funções de negócio;
- Providenciar a capacidade de verificar, remover, aprovar e certificar privilégios e/ou *roles* atribuídas a utilizadores;
- Analisar e auditar o histórico de acessos efetuados por uma identidade.

Framework A *framework* de Gestão de Identidades e Acessos da *EY*, representada em 3.1, apresenta-nos uma visão holística de todos os componentes, conceitos e definições que constituem uma gestão de identidades e acessos eficiente. A *framework* apresentada divide-se em cinco grandes domínios: *governance*, identidades e credenciais, acessos, fontes de autoridade e admistração e inteligência.

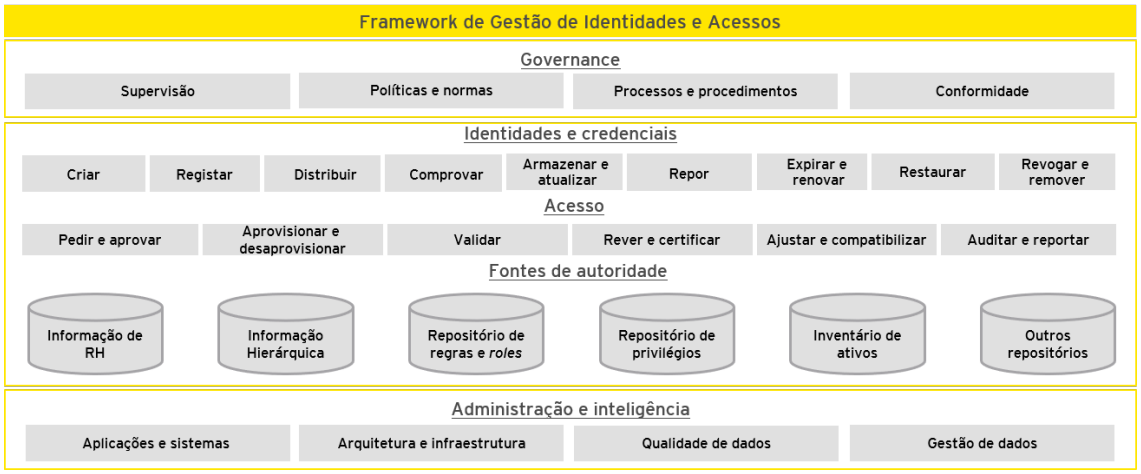

Figura 3.1: *Framework* de Gestão de Identidades e Acessos da EY

3.1.1 *Governance*

O domínio de *governance* assume-se como o alicerce do programa de gestão de identidades e acessos, fornecendo uma supervisão global e uma *framework* de governo para a gestão de identidades, relativamente a pessoas, processos e tecnologias. Este domínio descreve o alinhamento estratégico da organização e define as funções e responsabilidades dos

principais *stakeholders* associados ao programa de gestão de identidades e acessos. Os conceitos base do domínio de *governance* são:

- **Supervisão**: providencia a estratégia de gestão de identidades e acessos e assegura o envolvimento da liderança da organização no programa.
- **Políticas e normas**: processos usados para criar, validar, atualizar e comunicar as políticas que dão forma aos procedimentos e ferramentas usadas para implementar o programa de gestão de identidades e acessos.
- **Processos e procedimentos**: define um conjunto ordenado de atividades usado para criar, validar, atualizar e comunicar regras que gerem vários aspetos do programa, e/ou desenvolvimento e operação da solução.
- **Conformidade**: processos e ferramentas utilizadas para avaliar o grau de conformidade para com os regulamentos, políticas e normas definidas.

3.1.2 Identidades e Credenciais

Entende-se por identidade, o conjunto de caraterísticas pelas quais um utilizador é reconhecido. Nesta *framework*, uma identidade é representada por um perfil de identidade, constituído por um identificador único e um conjunto de atributos que descrevem o utilizador (nome, número de empregado, departamento, nome do gestor responsável, etc). As atividades que constituem este domínio são:

- **Criar**: processos, normas e ferramentas associadas com a criação de identificadores, perfis de identidade e credenciais.
- **Registar**: processos, normas e ferramentas associadas utilizadas para inserir os identificadores, perfis de identidade e credenciais no sistema alvo.
- **Distribuir**: processos e ferramentas utilizadas para comunicar ou transferir as credenciais para o utilizador apropriado de forma segura.
- **Comprovar**: processos e ferramentas utilizadas para comprovar identidades.
- **Armazenar** e **atualizar**: processos, normas, ferramentas e repositórios associados ao armazenamento e manutenção de credenciais e dados de utilizadores.
- **Repor**: processos e ferramentas necessárias para desativar e substituir credenciais (esquecidas).
- **Expirar** e **renovar**: processos, normas e ferramentas associadas com suspensão e reativação de credenciais após uma duração específica.
- **Restaurar**: processos e ferramentas usadas para eliminar credencias perdidas ou roubadas e fornecer credenciais de substituição.

- **Revogar** e **remover**: processos e ferramentas usadas para desativar ou apagar credenciais.

3.1.3 Acessos

O domínio de acessos inclui os processos e ferramentas responsáveis pela solicitação e respetiva aprovação/negação de privilégios de acesso a recursos protegidos. Os componentes incluídos neste domínio refletem o ciclo de vida da gestão de acessos:

- **Pedir e Aprovar**: processo de solicitação e aprovação de um acesso a um utilizador. Isto inclui todos os processos e ferramentas responsáveis por transmitir o pedido ao aprovador apropriado, registar a sua decisão e encaminhar o pedido para a próxima fase de processamento baseada nas decisões do aprovador.
- **Aprovisionar e desaprovisionar**: processo responsável por atribuir o acesso à aplicação ou sistema a um utilizador. O desa-provisionamento de acessos pode ser despoletado devido a várias razões, como ocorrências ao nível dos recursos humanos (despedimento ou mudança de função).
- **Validar**: processo responsável por validar os privilégios do utilizador aquando da tentativa de acesso ao recursos alvo.
- **Rever e certificar**: este processo inclui a definição das entidades responsáveis por rever e certificar os acessos, de forma a confirmar que todos os privilégios atribuídos estão em conformidade com as funções desempenhadas pelo utilizador.
- **Ajustar e compatibilizar**: processo responsável por corrigir as discrepâncias entre os privilégios aprovados e os privilégios que se encontram atualmente atribuídos nas aplicações.
- **Auditar e reportar**: o processo responsável pela produção e extração de *logs*, de forma a possibilitar a auditoria por parte de utilizadores autorizados.

3.1.4 Fontes de autoridade

Domínio da *framework* responsável pela criação e manutenção de toda a informação referente à gestão de identidades e acessos. Alguns exemplos de repositórios são:

- **Repositório de identidades**: repositório responsável por armazenar e gerir a informação de identidades.
- **Repositório de privilégios**: repositório responsável por armazenar os privilégios atribuídos aos diversos utilizadores e registar informação relativa aos mesmos (data de pedido, aprovação, inicio e fim).
- **Inventário de ativos**: repositório responsável por armazenar toda a informação referente aos ativos da organização.

3.1.5 Administração e Inteligência

A componente de administração da *framework* refere-se aos processos, aplicações e ferramentas usadas para garantir a gestão e manutenção dos elementos que constituem a solução de gestão de identidades e acessos. Estes sistemas incluem o sistema de pedido, aprovação e aprovisionamento; sistemas de revisão de acessos e identidades; sistemas e ferramentas de reconciliação; sistemas de autenticação e autorização; sistemas de monitorização; e fontes de autoridade.

A componente de inteligência refere-se aos processos e ferramentas utilizados para a análise de dados que compõe a gestão de identidades e acessos, tais como as identidades, privilégios, atividades do utilizador ou dados de acontecimento de risco.

Atividades relacionadas com este domínio incluem:

- **Análise de identidades e acessos**: a descoberta e análise de padrões resultantes dos dados sobre identidades e privilégios. Esta análise é muito útil na determinação de anomalias de acesso.
- **Registos de *logs* e monitorização**: os processos, normas e ferramentas associados à captura, agregação, correlação e análise de dados.
- **Produção de relatórios**: a capacidade de gerar e distribuir informações sobre a administração e operações dos componentes da solução aos vários intervenientes.

Nota: Como é possível verificar, a *framework* descrita, apesar de bastante completa e abrangente, acaba por incluir demasiados sub-domínios, que podem gerar confusão e resistência à mudança em empresas de menor dimensão, devido à ausência de conhecimento que apresentam sobre o tema em questão.

No capítulo seguinte podemos observar uma proposta de adaptação da *framework* global da EY, ao contexto nacional.

Capítulo 4

Análise realizada

Embora à data de conclusão da presente dissertação o projeto continue em curso, foi possível analisar e realizar a maioria dos passos propostos no âmbito do mesmo.

Fruto da experiência e *feedback* adquirido por parte, tanto dos membros da equipa como da organização em que este se insere, será apresentado neste capítulo um conjunto de recomendações a ter em conta em projetos futuros.

4.1 Alterações à *framework* de gestão de identidades e acessos

Nesta secção serão apresentadas as alterações realizadas à *framework* original e a respetiva *framework* resultante (figura 4.1). Estas foram efetuadas com vista a reduzir o número de sub-domínios apresentados e a tornar a nomenclatura mais acessível para todas as partes envolvidas.

- Os sub-domínios **Criar** e **Registar** do domínio **Identidades e credenciais** deverão ser aglomerados devido às parecenças que apresentam. Desta aglomeração, resulta o sub-domínio **Gerar**, que passa a incluir todos os processos e ferramentas associadas à criação de perfis de identidade, e respetivas credenciais, nos sistemas alvo.

- Os sub-domínios **Repor** e **Restaurar** deverão ser descartados e as respetivas contribuições adicionadas ao sub-domínio **Renovar**. Este domínio passa a incluir todos os processos e ferramentas associadas à renovação de credenciais, seja esta fruto de esquecimento (**Repor**), perda ou roubo (**Restaurar**) e/ou de uma desativação automática após término do período de validade (**Renovar**).

- O sub-domínio **Armazenar e Atualizar** poderá também ser descartado, uma vez que as suas contribuições poderão ser distribuídas pelos vários subdomínios do domínio de Análise e administração.

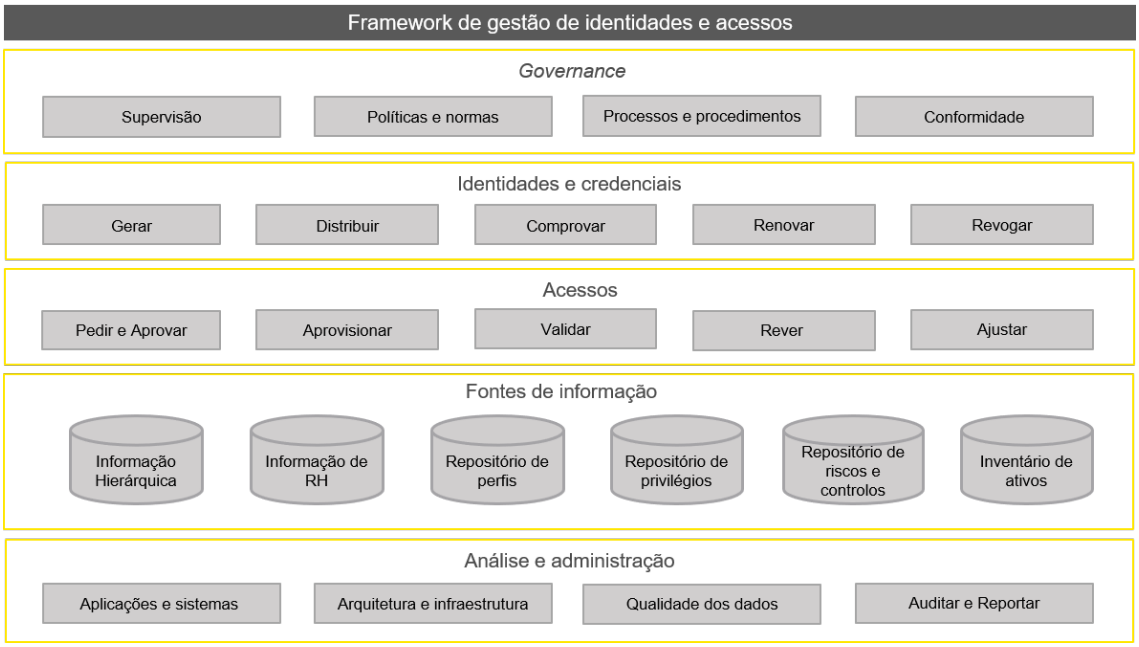

Figura 4.1: *Framework* de Gestão de Identidades e Acessos [Adaptada]

- O domínio de **fontes de autoridade** deve ser alterado para **fontes de informação**, de forma a aumentar o âmbito do mesmo. Deverá ser removido o repositório de regras e *roles* e adicionados dois novos repositórios: um repositório para o armazenamento de perfis funcionais e outro para armazenar informação referente a riscos e controlos mitigatórios. Como já se encontram representados os repositórios mais relevantes para a gestão de identidades e acessos o sub-domínio **Outros repositórios** poderá ser, eventualmente, descartado.

- O nome do último domínio deverá ser alterado para **Análise e Administração**, de forma a refletir melhor as responsabilidades inerentes ao mesmo.

- O sub-domínio, anteriormente pertencente ao domínio de acessos, **Auditar e Reportar**, deverá passar a integrar o domínio de **Análise e Administração**, de forma a englobar a análise tanto de acessos como de identidades. O sub-domínio **gestão de dados** poderá ser aglomerado ao sub-domínio **qualidade de dados**.

4.2 Definição da metodologia padrão

Durante a execução do projeto, foi possível verificar que alguns dos passos sugeridos *à priori* poderiam ser aglomerados ou, até mesmo, descartados, seja devido à ausência de benefícios concretos ou imediatos ou devido à sua longa duração e/ ou importância acrescida.

Foi possível verificar, por exemplo, que o passo de identificação de soluções tipo para cada *cluster* encontrado envolve demasiado tempo e esforço associados, tendo em conta

os benefícios apresentados.

Durante o processo de clusterização de todos os atributos foi possível perceber que os *cluters*/grupos mais importantes serão, geralmente, baseados em atributos como o tipo de autenticação e o tipo de gestão de acessos apresentada pela aplicação (ex: perfis aplicacionais, permissões de base de dados, etc). Outros atributos como o tipo de tecnologia utilizada no desenvolvimento ou a tecnologia de base dados, embora relevantes, não influenciam de igual forma o programa de gestão de identidades e acessos.

A revisão de contas adormecidas de utilizadores/acessos privilegiados, por outro lado, apresenta-se como um passo de extrema importância para uma gestão de acessos eficaz. Dada a sua relevância, este deve ser realizado num projeto em separado, em paralelo à fase de implementação do modelo e não durante a fase de diagnóstico.

Tendo em conta a referida análise e, de forma a facilitar a compreensão por parte de todos os intervenientes do programa de gestão de identidades e acessos, a metodologia sugerida será constituída por 4 grandes fases:

- **Fase de diagnóstico**: Durante a fase de diagnóstico é efetuada a identificação e análise do portfólio aplicacional, o levantamento das ferramentas de suporte e dos mecanismos de autenticação existentes e, por último, a análise do modelo de governo atual e processos de gestão de acesso em vigor. No capítulo 5, encontram-se descritos os passos a realizar durante a referida fase. Será também apresentada, como exemplo, a análise de maturidade efetuada à empresa X.

- **Fase de definição do modelo**: Tendo em conta o estado atual da organização, a fase seguinte passa pela definição do modelo de governo a aplicar e pela definição de normas e processos a seguir. O capítulo 6 descreve o modelo de gestão de identidades e acessos proposto. Neste são apresentados *guidelines* e controlos úteis para a definição do mesmo.

- **Fase de definição do *roadmap***: Após a definição do modelo e do estádio ideal de maturidade a alcançar, é necessário definir o caminho a seguir e as iniciativas necessárias para alcançar o objetivo pretendido. As iniciativas propostas encontram-se descritas no capítulo 7.

- **Fase de implementação:** Por último, o modelo de gestão de identidades e acessos deverá ser implementado na organização, com ou sem o auxílio de uma ferramenta de suporte associada. A fase de implementação não se encontra contemplada na presente dissertação.

Capítulo 5

Fase 1 - Diagnóstico

5.1 Identificação e caraterização do portfólio

Numa primeira fase, de forma a analisar a situação atual da organização, é necessário efetuar o levantamento de todo o seu portfólio aplicacional, que se encontra, muitas das vezes, dividido pelas várias áreas que a constituem.

Para identificar de forma eficaz todo o portfólio, as áreas deverão ser entrevistadas de modo a levantar todas as aplicações desenvolvidas e/ou utilizadas pelos seus membros, e aferir o modelo de gestão de identidades e acessos utilizado por cada uma delas.

Durante o processo de levantamento, é imprescindível definir um conjunto de critérios e/ou atributos que abranjam a maioria das caraterísticas inerentes às aplicações existentes na organização, para que estas sejam classificadas corretamente.

O conjunto definido assenta em 4 grupos de caraterísticas: contexto da aplicação, ficha técnica, gestão de identidades e acessos e por último, controlo de acessos.

A. Contexto da aplicação

- **Contexto**: histórico da aplicação, áreas e processos que suporta na organização.
- **Tipo de dados**: perceber se possui dados críticos para o negócio e/ou dados pessoais.
- **Acesso de terceiros**: perceber se é acedida por entidades externas.
- **Alterações previstas**: averiguar se aplicação irá permanecer sem alterações ou irá entrar em processo de substituição, descontinuação ou alteração.

B. Ficha técnica da aplicação

- **Sistema operativo (tipo e versão)**: Windows, AIX, Linux, Solaris, Android, iOS.
- **Tecnologia de base de dados (tipo e versão)**: Microsoft SQL, Oracle, MySQL, Mongo/Maria, PostgreSQL.
- **Framework Web/Mobile**: .net ASPX, Java, ReactNative, SharePoint, Oracle Forms, Outsystems, JavaScript.
- **Disponibilidade**: Interna ou exposta para o exterior.
- **Vocação**: Interna ou para uso de clientes.

C. Gestão de identidades e acessos

- **Identidade**: perceber de que forma são criados os utilizadores, manualmente pelas equipas de administração de sistema, através de funcionalidades *self-service*, ou com ajuda de uma ferramenta de gestão de identidades e acessos; e de que forma são geridas as identidades de colaboradores, fornecedores e/ou clientes e respetivas fontes de informação.
- **Gestão de acessos**: averiguar de que forma se encontram definidos os processos de gestão de acessos de colaboradores e fornecedores, como por exemplo, processos que descrevem os atos de solicitar, aprovar, modificar, remover e rever acessos;
- **Ferramentas**: identificar se existem ferramentas na organização que servem de suporte ao processo de gestão de acessos da aplicação (ex: ferramenta de *ticketing* de suporte à gestão de serviço, ITSM).

D. Controlo de acessos

- **Autenticação**: identificar de que modo é feita a autenticação na aplicação (local, centralizada, federada), quantos fatores são utilizados, qual o protocolo escolhido e de quer forma esta comunica com outros sistemas. Estes conceitos encontram-se descritos nas secçoes, 2.5, 2.3.4 e 2.3.3, respetivamente.
- **Perfis**: Quando aplicável, identificar de que modo se encontram definidos os perfis de acessos e qual a sua granularidade. Os principais modelos de controlo de acessos encontram-se descritos na secção 2.4.3.

5.2 Análise de maturidade da organização

Com base na *framework* adaptada, apresentada na figura 4.1, cada subdomínio é avaliado de 1 a 5 tendo em conta o nível de maturidade que apresenta. Desta forma, uma análise efetuada com recurso a esta *framework* permite avaliar o nível corrente de maturidade da organização, servindo este de base para a definição pragmática do *roadmap* a seguir, de forma a alcançar o nível de maturidade futura pretendido.

Contudo, uma organização nem sempre deve tentar alcançar os níveis mais altos de maturidade em cada componente. O nível de maturidade desejado deve ser baseado em algumas das seguintes considerações:

- Objetivos e necessidades de negócio;
- Requisitos de conformidade regulamentar;
- Tolerância ao risco;
- Magnitude aceitável de mudança que a organização está disposta ou é capaz de suportar;
- Custo/benefício da implementação.

Uma gestão de identidades e acessos eficaz passa por definir, de forma clara, o nível de maturidade que se pretende alcançar, de forma a controlar as expetativas de todos os intervenientes do programa e a chegar a um consenso sobre a definição de um *roadmap* pragmático a seguir com vista a alcançar os objetivos esperados.

5.2.1 Exemplo de análise de maturidade - *Framework* adaptada

A figura 5.1 apresenta, de forma gráfica, os resultados obtidos após a realização da análise de maturidade da empresa X, recorrendo à *framework* adaptada.

Os domínios com maturidade reduzida estão maioritariamente relacionados com a ausência de políticas, normas, processos e/ou procedimentos relacionados com a gestão de identidades e acessos. Por norma, existe visibilidade limitada quanto aos privilégios acumulados em cada utilizador da organização, que muitas das vezes possuem acessos de teor privilegiado e/ou acessos em conflito de segregação de funções.

Os processos de revisão de contas são esporádicos ou inexistentes, assim como as retificações de privilégios atribuídos aquando de uma alteração de funções do colaborador ou da sua saída da organização.

Governance O domínio de *Governance* apresenta-se como um dos mais importantes, servindo de base a toda a estrutura necessária para o bom funcionamento do programa de gestão da organização. É neste domínio que se encontram muitos dos principais problemas que põem em causa a sua eficiência.

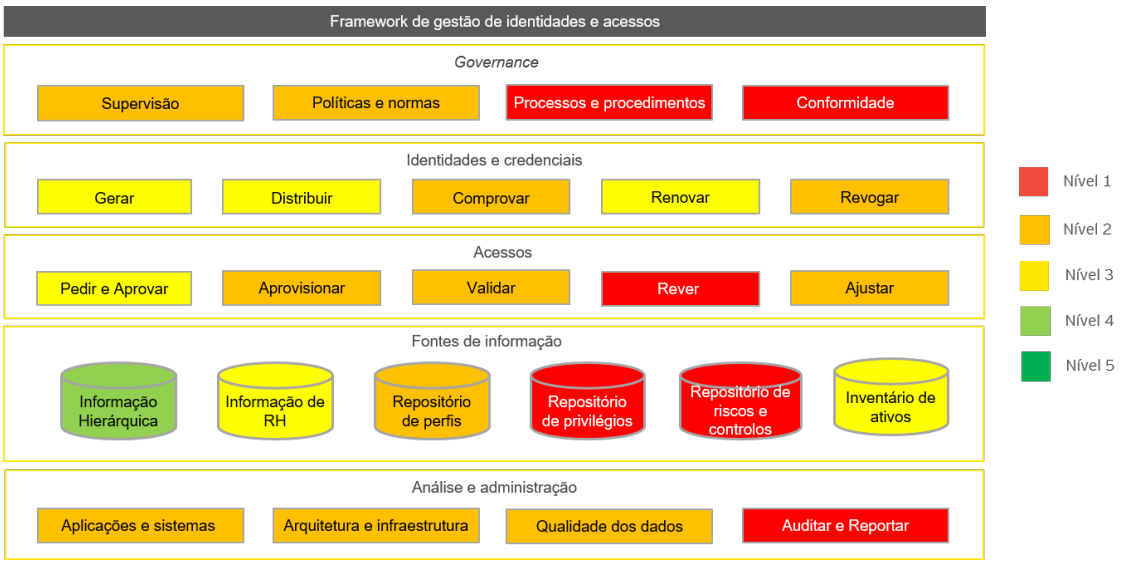

Figura 5.1: Análise de maturidade atual - empresa X

Os principais obstáculos passam pela ausência de um programa efetivo de *governance* e pela falta de interesse e/ou apoio dos membros executivos que constituem a liderança da organização. Dada a ausência de responsabilidades definidas, a gestão de identidades e acessos encontra-se, por norma, atribuída aos colaboradores da área TI, que, muitas vezes, não possuem a experiência ou visibilidade de negócio necessária para tomar decisões ou para entender os riscos associados às suas práticas.

Na análise efetuada à empresa X, foi possível verificar exatamente isso, a estratégia de gestão de identidades e acessos não se encontra formalmente definida e não é adotada de forma transversal pela organização. O governo de identidades e acessos é normalmente gerido em silos funcionais, existindo entre as áreas, diferentes processos de gestão de acessos. A ausência de políticas de gestão de identidades e acessos que sejam aplicadas transversalmente, resulta na ausência de *standards* processuais e na presença de vários procedimentos díspares ao longo das várias áreas funcionais, limitando a visibilidade sobre a realidade existente.

Os pedidos de criação de utilizadores podem, por exemplo, ser realizados via *e-mail*, apoio a cliente ou plataforma ticketing de gestão (*ITSM*). O mesmo se verifica com os processos de distribuição de credenciais, podendo os mesmos ser realizados via correio, *e-mail*, telefone ou presencialmente.

Os processos informais existentes na organização não consideram uma análise de risco, não existindo medidas mitigatórias em caso de ações que comportam um risco elevado. Não existem procedimentos de conformidade, dado não existirem políticas inerentes à gestão de identidades e acessos em vigor na organização.

Identidades e Credenciais Durante a análise ao domínio de gestão de identidades encontramos desafios como: a existência de vários repositórios de utilizadores para autenticação e autorização a nível local, levando a uma visibilidade reduzida de acessos por identidade; e uma gestão de ciclo de vida da identidade deficiente, não existindo um processo de atribuição de credências automático no *onboarding* de novos utilizadores, nem de revogação de todas as credenciais afetas à identidade aquando de uma saída.

As responsabilidades de revisão de identidades e credenciais, muitas das vezes, não se encontram atribuídas, devido à ausência de uma programa de gestão de identidades e acessos definido.

De forma a perceber melhor os desafios encontrados, podemos analisar alguns exemplos de casos de uso, observados na empresa X, referentes ao domínio da gestão de identidades:

- **Criação de conta na Active Directory:** Aquando da entrada de um colaborador na empresa X, é-lhe atribuída uma conta na *Active Directory* (AD), acompanhada por um endereço de *e-mail* e um número de colaborador que serve como identificador único do utilizador (figura 5.2). Este identificador é utilizado como referência em algumas das aplicações, sendo possível correlacionar esta chave ao longo dos sistemas da empresa X.

  Adicionalmente, neste processo de entrada, é gerada automaticamente uma *password* com complexidade alinhada com a indústria.

  Relativamente a colaboradores externos, e dependendo das necessidades de acesso, pode também ser solicitada a criação de conta na AD, como observado na figura 5.3.

  Apesar de existir um esforço da organização no sentido de promover a ligação/sincronização de aplicações à AD, muitas delas continuam a reger-se por um processo de criação de credenciais local. Nestes casos, é utilizado o número de colaborador (identificador) como nome de utilizador na aplicação e é gerada uma *password* específica para a aplicação em causa (distinta da *password* utilizada nas credenciais globais do utilizador).

- **Criação e comunicação de credenciais de acesso:** No registo de utilizadores, para as aplicações não integradas com a AD, os pedidos de criação de credenciais de acesso são, na sua maioria, efetuados via ITSM. Neste processo de criação de credenciais é, por norma, utilizado o *global ID* do colaborador acompanhado pela *password* de acesso. Estas são, na maioria das aplicações, *passwords* de complexidade reduzida, não estando em linha com práticas correntes de mercado.

  A comunicação de credenciais é realizada por diferentes canais, não existindo um *standard* ao longo das diferentes áreas funcionais. A nível da AD, as credenciais podem ser enviadas via carta ou via *e-mail* para as chefias sempre que são pedidos urgentes. No caso das credenciais de aplicações não integradas com a AD, estas são normalmente comunicadas via *e-mail* ou telefone.

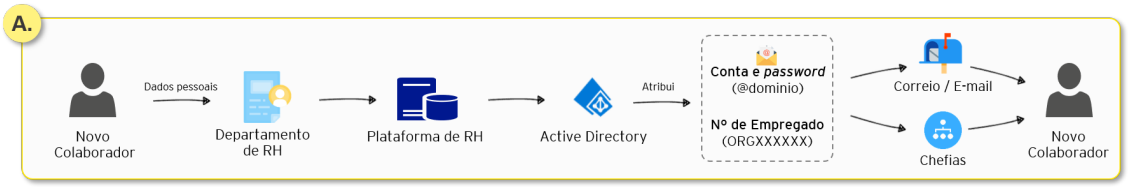

Figura 5.2: Criação de credenciais para colaboradores internos

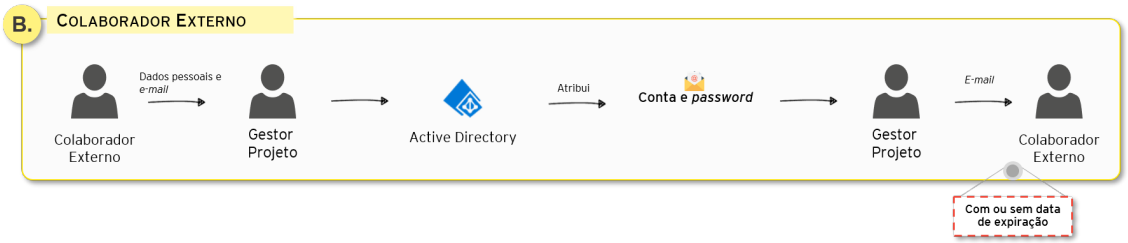

Figura 5.3: Criação de credenciais para colaboradores externos

- **Gestão de *passwords*:** Sempre que é necessário efetuar um *reset* à *password*, nas aplicações em que esta funcionalidade não se encontra disponível através de *self-service*, podem ser usados vários canais para o fazer (ex.: via ITSM, *e-mail*, telefone). Não existem procedimentos definidos para comprovação da identidade. Os processos de expiração de *passwords* apenas existem para contas na AD, onde existe um processo de renovação de *passwords* a cada 90 dias.

- **Revisão e revogação de credenciais:** O processo de revogação de credenciais apenas existe no caso da AD e, por consequência, nas aplicações que estão integradas na mesma. Não existe um processo de revogação de credenciais de acesso para aplicações com autenticação local. Adicionalmente, verificou-se a ausência de um processo de revisão de utilizadores em grupos na AD. Existe um processo de revisão de utilizadores informal em algumas aplicações, levado a cabo ocasionalmente, motivado por questões de licenciamento.

Acessos No domínio da gestão de acessos podemos encontrar situações em que:

- Os pedidos de acesso são aprovados sem análise de risco de segregação de funções ou de acesso privilegiado;

- Utilizadores possuem privilégios excessivos, pondo em causa os princípios *implicit deny* e *least privilege* (2.4.2);

- O tempo de espera entre o pedido de privilégios e a sua atribuição é elevado;

- A atribuição de privilégios é realizada à medida ou através da clonagem dos privilégios atribuídos a outro utilizador;

- Os acessos aplicacionais não são usualmente revistos com base em alterações da situação do colaborador (alteração da função ou saída do colaborador), pondo em causa o princípio *Need to know* (2.4.2);

- As revisões de privilégios, quando ocorrem, são motivadas por questões de licenciamento.

De forma a perceber melhor os desafios encontrados, podemos analisar alguns exemplos concretos de casos de uso, observados na empresa X, referentes ao domínio em questão:

- **Entrada de novo colaborador:** Na empresa X foi observado que, aquando da entrada de um novo colaborador, o processo de requisição de acessos não é despoletado de forma automática. Os pedidos de acessos são apenas realizados após criação do cadastro do colaborador na plataforma de recursos humanos, podendo resultar numa maior demora no acesso a aplicações para o desempenho da sua função.

  A requisição de acesso é, por norma, realizada através da abertura de *ticket* na plataforma *ITSM*, seguindo um processo de aprovação *standard*, conhecido ao longo da organização. Contudo, existem casos em que os pedidos não são formalizados, resultando numa menor rastreabilidade dos pedidos (ex.: pedidos feitos diretamente ao *key user*, via *e-mail* ou presencialmente). Na figura 5.4 encontra-se representados os casos acima referidos.

- **Solicitação de privilégios:** Existem diversos tipos de fluxos para os pedidos de acessos, dependendo da eventual necessidade de licenciamento do utilizador. Para pedidos com necessidade de licenciamento, este é avaliado pelos superior hierárquico ou *key user* e pelos diretores de 1ª linha e de SI. Para pedidos sem necessidade de licenciamento, o pedido é analisado apenas pelo *key user* da aplicação. Em ambos os fluxos, não é realizada uma análise de segregação de funções ou avaliado o risco do pedido de acesso, limitada pela falta de visão holística dos acessos dos utilizadores.

- **Acesso de externos:** Existem acessos privilegiados atribuídos a parceiros externos, sem definição de medidas mitigatórias para riscos que advenham dos mesmos. A visibilidade quanto à utilização de contas privilegiadas é baixa, não existindo controlo e monitorização de atividades realizadas, nem renovação periódica de *passwords*. A gestão de externos é da responsabilidade de cada gestor de projeto, traduzindo-se em fontes de informação dispersas, sem que exista uma visão geral dos mesmos.

- **Acessos VPN:** Existe ainda um processo de criação de acesso VPN, sendo o mesmo iniciado via abertura de *ticket* na plataforma *ITSM*, com o preenchimento de um formulário posteriormente assinado pelo diretor de primeira linha.

- **Monitorização:** A ausência de *loggings* de acessos em algumas aplicações, assim como ausência de medidas de controlo e monitorização, não permite à empresa X monitorizar e avaliar possíveis falhas de segurança e pontos de melhoria. Não existem métricas de acompanhamento dos processos de gestão de identidades e acessos, não sendo possível averiguar possíveis constrangimentos ao longo do mesmo.

- **Revisão de acessos:** Atualmente, não existe um processo de revisão de acessos que garanta a atualização de acessos do utilizador aquando de uma alteração do estado/-funções do utilizador (ex.: quando um colaborador muda de funções são adicionados acessos aos que o utilizador já detinha não sendo removidos os antigos); ou processo de remoção de acessos aquando de uma saída da organização.

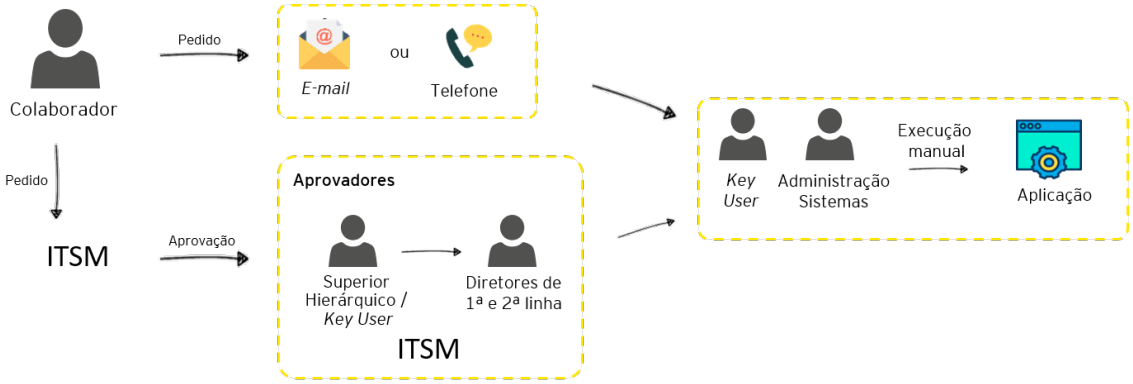

Figura 5.4: Pedido e atribuição de acessos

Fontes de informação Ao nível de fontes de informação, observamos que, para colaboradores internos, o processo de gestão de identidades encontra-se bem definido, sendo usualmente iniciado com o registo na plataforma de recursos humanos, que comunica, diariamente, à AD os dados dos colaboradores a serem integrados no sistema. A plataforma possui informação atualizada do colaborador.

Para colaboradores externos, o processo de gestão de utilizadores é da responsabilidade de cada gestor de projeto, traduzindo-se em fontes de informação dispersas, não existindo uma visão geral da identidade do colaborador externo. Esta descentralização pode potenciar a existência de informação desatualizada e falta de visibilidade sobre acessos (muitos destes privilegiados), podendo culminar em acessos indevidos por parte de colaboradores externos aos sistemas da empresa X.

Na maioria das aplicações, a gestão de utilizadores é realizada localmente em cada aplicação (sem integração com a AD), existindo uma falta de visão de acessos centralizada por utilizador, dificultando a identificação de acessos em situações onde seja necessário alterar ou remover os mesmos. Adicionalmente, não existe uma gestão de perfis adequada e centralizada, sendo esta realizada individualmente ao nível da base de dados ou da aplicação.

Análise e Administração Por último, verificamos que não existe uma arquitetura clara de gestão de identidades que centralize os processos do ciclo de vida dos utilizadores para todas as aplicações e sistemas, causando desalinhamentos processuais, duplicação de informação, aumento de irregularidades e limitando possíveis análises para fins de monitorização e auditorias de acessos.

Com recurso à AD, a empresa X tem vindo a trabalhar num modelo que poderá servir de repositório central à gestão de identidades e acessos. Contudo, a maioria das aplicações e sistemas da organização não estão integrados com este modelo, traduzindo-se na replicação de dados de utilizadores e, consequentemente, falta de um visão holística das identidades e acessos.

Apesar do esforço para mitigar a existência de contas partilhadas, existe uma falta de visibilidade sobre a utilização das mesmas, não existindo controlo e monitorização de atividades realizadas, nem renovação periódica de *passwords* ou revisão de utilizadores, conduzindo a uma baixa visibilidade e rastreabilidade dos acessos a estas contas. A ausência de *loggings* de acessos e de medidas de controlo e monitorização não permite à empresa X monitorizar e avaliar possíveis falhas de segurança e pontos de melhoria.

As credenciais são geridos de forma descentralizada, limitando a experiência do utilizador. A maioria das passwords passam por um processo de hash.

Capítulo 6

Fase 2 - Definição do modelo a aplicar

A gestão de identidades e acessos é conseguida através de uma definição clara de responsabilidades dos vários intervenientes (modelo de governo) e pela existência de diretrizes de suporte quer seja através da definição de políticas e normas ou da definição de processos que descrevem especificamente qual o fluxo de atividades, intervenientes e pontos de decisão. O enquadramento do modelo pode ser observado na figura 6.1.

Figura 6.1: Enquadramento do modelo

6.1 Princípios base do modelo

O modelo de gestão de identidades e acessos definido deverá ser suportado na existência de perfis funcionais, adaptados às necessidades de cada função na organização, o que permite agilizar o processo de *onboarding*, alteração e *offboarding*, na medida em que os mesmos são previamente analisados e aprovados por cada diretor de primeira linha.

Adicionalmente, este promove ainda uma visão única da identidade com informação de acessos e permissões centralizada através de um repositório de acessos.

O modelo inclui conceitos como:

- **Perfis funcionais**: Construção de perfis funcionais, *à priori*, baseado no modelo de controlo de acessos, *Role Base Access Control (RBAC)* e no princípio da segregação de funções, apresentados em 2.4.3 e 2.4.2, respetivamente, de forma a restringir os acessos da organização, tendo como base as funções desempenhadas pelos colaboradores.

  A construção de um perfil funcional passa por detalhar todas as aplicações necessárias ao desempenho da função e por mapear as atividades com as respetivas permissões existentes em sistema, incluindo um ou mais perfis aplicacionais existentes.

- **Aprovação por *default***: O processo de *onboarding* do colaborador é agilizado pelo facto de existir um perfil funcional por função desempenhada, que é atribuído assim que o colaborador entra na organização, não sendo necessário qualquer aprovação. Apenas a atribuição de utilizadores com acessos privilegiados será sujeita a aprovação do diretor de primeira linha da área.

- **Visão única da identidade**: A informação respeitante aos vários tipos de utilizadores encontra-se centralizada, permitindo uma gestão transparente e efetiva do ciclo de vida do utilizador. No caso de externos, gestores de projeto serão responsáveis por consolidar a informação em sistema, de forma a garantir que a gestão de identidade de colaboradores externos se encontra atualizada.

- **Repositório de privilégios**: Um repositório de acessos e permissões por identidade irá permitir ter uma visão agregada dos acessos na organização, facilitando o processo de remoção e alteração de acessos, assim como monitorização e auditorias de acessos, permitindo identificar exceções às normas e processos definidos, assim como aferir o risco inerente.

6.2 Modelo de governo

O modelo de governo define a estrutura e responsabilidades inerentes a todos os componentes do modelo gestão de identidades e acessos, e respetiva articulação entre estes.

A presente secção define um modelo de governo genérico de gestão de identidades e acessos, que poderá ser adaptado a qualquer organização, considerando o organograma existente. *Frameworks* internacionais como o *COBIT* [10], apresentam boas práticas úteis para a definição do mesmo.

6.2.1 Comités e equipas

O modelo de governo é constituído por dois comités de cariz estratégico (Comité Executivo e Comité de *Governance* de Gestão de Identidades e Acessos) e quatro equipas de cariz operacional (Identidades, Acessos, Monitorização e Gestão de Perfis). A figura 6.2, representa de uma forma gráfica a referida constituição.

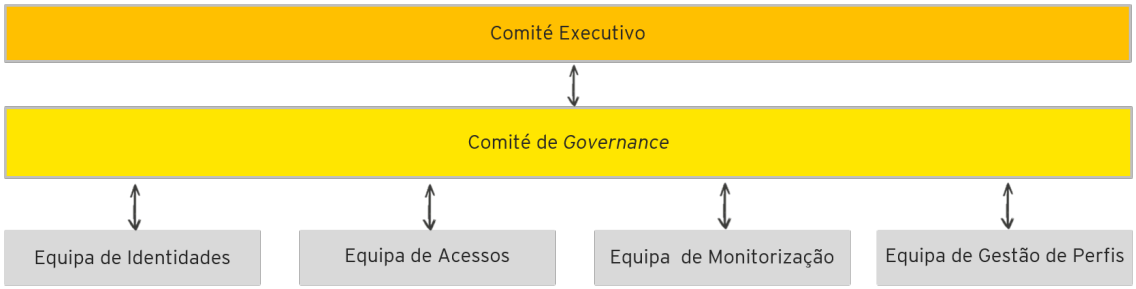

Figura 6.2: Comités e equipas do modelo de governo

- **Comité Executivo**: O Comité Executivo tem como principal objetivo definir a orientação estratégica para o programa de gestão de identidades e acessos, atuar como entidade supervisora do programa e garantir a disponibilidade dos recursos adequados para as iniciativas a desenvolver.

- **Comité de *Governance***: É responsável pela supervisão das várias iniciativas a serem desenvolvidas, realizando revisões contínuas ao modelo e priorizando as iniciativas e projetos de acordo com o seu risco e criticidade para o negócio. É responsável ainda pela coordenação da comunicação de todos os participantes e por monitorizar a sua execução.

- **Equipa de identidades**: Responsável pela definição e gestão de processos que assegurem que as identidades dos utilizadores são definidas e geridas no ambiente da organização, suportando todo o seu ciclo de vida (criação, suspensão, alteração e remoção).

- **Equipa de acessos**: Responsável pela definição e gestão de processos de aprovisionamento e desaprovisionamento de acessos e permissões dos utilizadores a sistemas/aplicações.

- **Equipa de Monitorização**: Responsável pela definição e gestão de processos e sistemas que permitam à organização identificar, analisar e conciliar informação inerente a identidades e acessos, permitindo identificar situações de não conformidade.

- **Equipa de Gestão de Perfis**: Responsável pela definição e gestão de perfis funcionais e aplicacionais, tendo em consideração riscos e controlos mitigatórios. Fornece o suporte necessário à sua implementação.

6.2.2 Membros

Fazem parte destas equipas, interlocutores de perfil funcional com conhecimento do negócio, nomeadamente ao nível de processos e riscos, e interlocutores com perfil mais técnico, com conhecimento das diferentes aplicações, acessos e permissões, e respetivos impactos.

Diretor de primeira linha colaborador com funções de gestão, diretamente acima dos colaboradores com funções mais operacionais. Os diretores de primeira linha são geralmente responsáveis por gerir e supervisionar as tarefas realizadas pelos seus membros de equipa.

No âmbito da gestão de identidades e acessos, um diretor de primeira linha terá como responsabilidades a aprovação de perfis funcionais e aplicacionais, aprovação de pedidos de acessos privilegiados ou acessos de emergência (figura 6.3).

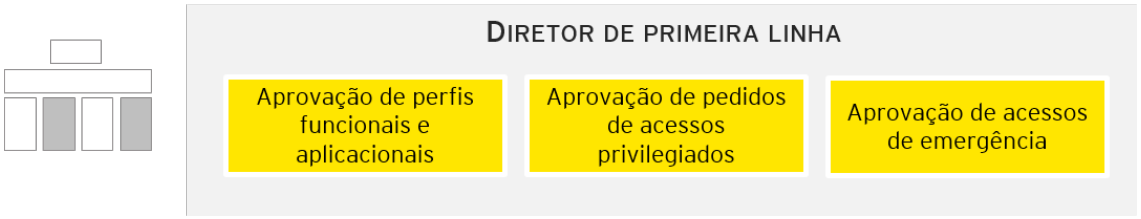

Figura 6.3: Responsabilidades do diretor de 1ª linha

***Key user* funcional** Um *key user* é um colaborador que possui bastante experiência e conhece a organização como nenhum outro. Este sabe que tipo de atividades devem ser desempenhadas por colaborador ao longo de um determinado processo, permitindo mapear com as respetivas autorizações em sistema; e percebe de que forma as mesmas se relacionam com outros departamentos, sendo um especialista em determinados processos.

No âmbito da gestão de identidades e acessos, consideramos a existência de pelo menos um *key user* por função efetuada na organização. As suas funções neste modelo de governo encontram-se identificadas na figura 6.4.

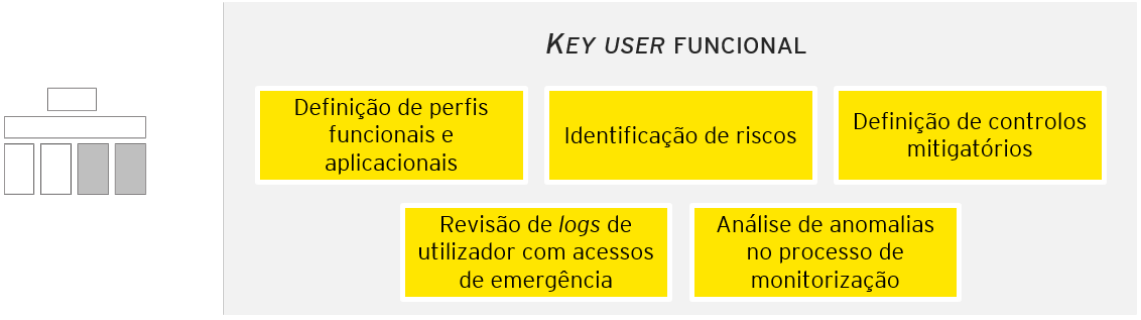

Figura 6.4: Responsabilidades do *key user* funcional

Gestão de risco Equipa responsável por monitorizar e analisar situações de risco e aprovar controlos mitigatórios propostos por outras entidades (figura 6.5).

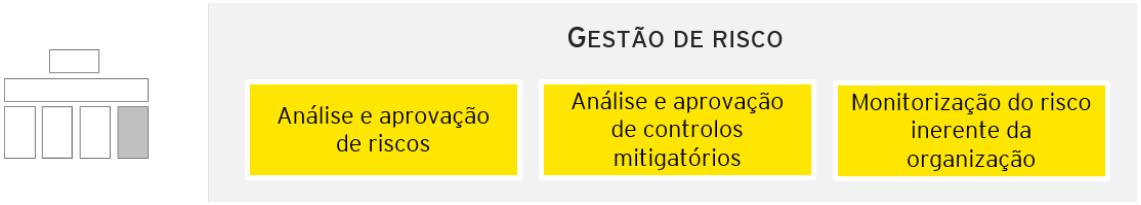

Figura 6.5: Responsabilidades da equipa de gestão de risco

Gestão de identidades Equipa constituída maioritariamente por profissionais de recursos humanos, responsáveis por gerir as plataformas existentes na organização (figura 6.6).

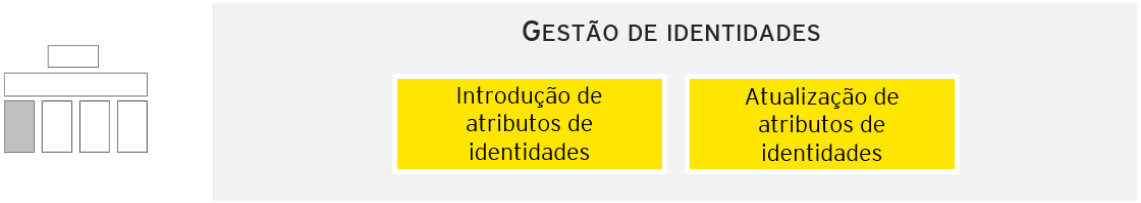

Figura 6.6: Responsabilidades da equipa de gestão de identidades

Responsável pelo repositório de privilégios Equipa constituída por um ou mais elementos responsável pela manutenção do repositório de privilégios. Este contém informação de todos os perfis (acessos e permissões) existentes, bem como de todos os perfis atribuídos a cada utilizador, de forma a recolher toda a informação relevante num só ponto de contato, construindo uma visão centralizada no utilizador (figura 6.7).

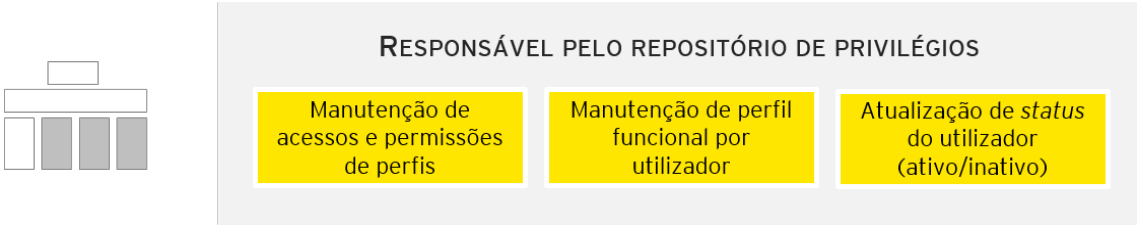

Figura 6.7: Responsabilidades da equipa responsável pelo repositório de privilégios

Manutenção aplicacional Equipa responsável pela manutenção e/ou desenvolvimento das aplicações que constituem o portfólio da organização. Responsáveis por analisar a viabilidade dos pedidos de criação/remoção de novas permissões e funcionalidades e pelo seu desenvolvimento/parametrização, sempre que aplicável (figura 6.8).

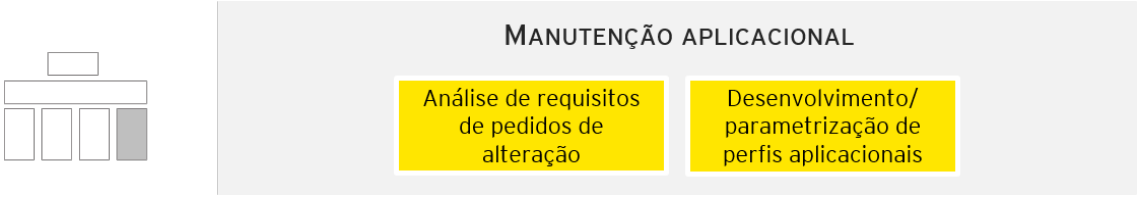

Figura 6.8: Responsabilidades da equipa de manutenção aplicacional

Administração de sistemas Equipa responsável pela gestão do sistema de diretoria existente na organização (ex: Active Directory) e pela atribuição/remoção de acessos e permissões às aplicações conectadas a este (figura 6.9).

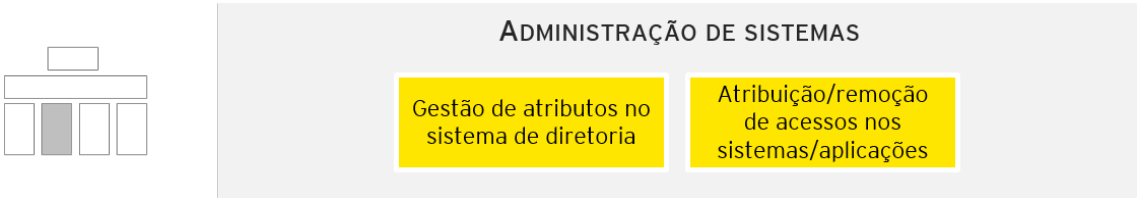

Figura 6.9: Responsabilidades da equipa de administração de sistemas

6.3 Políticas e normas

Os sistemas de informação são determinantes na atividade, eficiência e competitividade das organizações. É uma obrigação legal, ética e fundamental para o negócio assegurar a confidencialidade, integridade e disponibilidade da informação (2.1). A definição de políticas e normas permite definir controlos e diretrizes que assegurem a conformidade para com estes princípios fundamentais da segurança da informação.

No âmbito da gestão de identidades e acessos deverão ser criadas, como ponto de partida, duas normas que derivam da politica global da segurança da informação, a norma para *passwords* e a norma de gestão de identidades e acessos. Alguns dos controlos identificados pelas normas que se seguem são baseados no capítulo 9, Controlo de acessos, da norma de segurança ISO 27002 [19].

- **Política global da segurança de informação:** Constitui o principal pilar da segurança da informação de uma organização e estabelece uma base de entendimento comum, para todas as entidades da mesma, determinando os requisitos mínimos para a segurança da informação do grupo.

- **Norma de gestão de identidades e acessos:** Fornece um conjunto de diretrizes para criação e gestão das contas dos colaboradores. Define controlos e requisitos formais para o controlo de quem acede às aplicações, quais os seus privilégios e permissões e de que forma os mesmos são criados, atribuídos, geridos e removidos.

- **Norma para *passwords*:** Define os requisitos mínimos no que respeita à gestão de *passwords* utilizadas para acesso aos sistemas e/ou aplicações. Fornece um conjunto de diretrizes para assegurar a proteção de *passwords* e permitir a transmissão e alteração das mesmas de forma segura.

6.3.1 Norma para *passwords*

As *passwords* representam um dos pontos de falha mais explorado na tentativa de acesso não autorizado, inclusivamente a partir do interior das organizações.

Para que as *passwords* sejam um mecanismo eficaz na segurança de uma organização, é essencial que estas sejam selecionadas, armazenadas e geridas adequadamente. *Passwords* escolhidas de forma inadequada podem ser facilmente descobertas e posteriormente utilizadas para acessos não autorizados. Do mesmo modo, *passwords* que sejam armazenadas de modo inadequado estão sujeitas a revelação e utilização indevida por parte de pessoas não autorizadas.

Escolha de *passwords* Devem ser escolhidas *passwords* fortes com pelo menos 8 caracteres e uma mistura de letras maiúsculas, minúsculas, números e caracteres especiais. Estas devem ser fáceis de relembrar, não devem incluir informação pessoal facilmente acessível,

não devem conter palavras conhecidas de forma a evitar ataques dicionários e não devem apresentar sequências alfa-numéricas ([19], 9.3.1, D).

Proteção de *passwords* As *passwords* são pessoais e intransmissíveis, não devendo ser reveladas a ninguém, incluindo equipas de suporte e de administração, seja por intermédio de conversa, telefone, correio eletrônico ou quaisquer outros meios de comunicação ([19], 9.3.1, A). Somente a equipa responsável pela segurança poderá autorizar a partilha de *passwords*, após pedido por escrito, onde constem os motivos da necessidade de partilha.

Não devem ser usadas *passwords* nas contas de acesso aos sistemas que sejam semelhantes a contas de acesso de outras organizações e/ou contas pessoais ([19], 9.3.1, G). Quando possível, não deve ser usada a mesma *password* para vários sistemas da organização.

Deverá existir um registo central de *passwords* de administração de sistemas, equipamentos informáticos e aplicações para recuperação em caso de desastre. Este registo deverá ser classificado de acordo com a norma de classificação da informação em vigor na organização, e arquivado em local próprio e seguro. O controlo de acesso a essa informação deve acompanhar a sua classificação e criticidade.

Transmissão de *passwords* Quando autorizada pelas entidades competentes, a transmissão de *passwords* deve respeitar determinados requisitos de segurança, tendo em conta o meio através da qual é efetuada a mesma:

- **Via eletrónica**: as *passwords* não devem ser transferidas em claro ([19], 9.2.4, D) e deve ser garantida a utilização de uma técnica criptográfica segura e aprovada.
- **Via escrita**: quando for necessário fornecer uma password através de escrita, o destinatário deve tomar medidas de precaução de modo a não permitir acessos não autorizados (ex. depois de memorizar a *password*, o papel deve ser destruído).
- **Via oral**: em caso de transmissão oral de *passwords*, devem ser tomadas as devidas precauções para garantir que a comunicação não é ouvida por pessoas não autorizadas.

Alteração de *passwords* Sempre que seja necessário efetuar a alteração/reset de *passwords*, devem existir mecanismos que verifiquem, *à priori*, a identidade do utilizador ([19], 9.2.4, C). Caso alguns dos seguintes eventos ocorra, a alteração da *password* deve ser obrigatória:

- Criação de uma *password* temporária pela equipa de administração de sistemas (ex.: criação de uma nova conta de acesso, definição de uma nova *password*). Para este caso a palavra passe deve ser trocada após a primeira autenticação no sistema ([19], 9.3.1, D);

- Fim da validade atribuída a uma *password*;
- Comprometimento de um sistema em que a conta esteja a ser utilizada ([19], 9.3.1, C);
- Transmissão insegura de uma *password* (ex: via *e-mail* ou *chat*);
- Fornecimento ou revelação acidental da *password* a uma pessoa não autorizada.

Na aquisição de um novo sistema ou *software*, as *passwords* de origem devem ser alteradas de imediato.

6.3.2 Norma de gestão de identidades e acessos

A norma de gestão de identidades e acessos tem como objetivo fornecer um conjunto de diretrizes para controlo dos acessos lógicos aos sistemas, aplicações e informação da organização. Neste documento encontram-se definidos os controlos para as atividades relacionadas com a atribuição, modificação, desativação, reativação ou remoção de acessos.

Criação e gestão de contas de utilizadores A cada colaborador deve ser atribuído um identificador único (ex: número de colaborador ou *e-mail*) que o identifique perante os sistemas de informação da organização, de forma a assegurar a rastreabilidade das suas ações ([19], 9.2.1, A). Os identificadores de antigos colaboradores não podem voltar a ser reutilizados, de forma a garantir a existência de histórico de ações realizadas por utilizador ([19], 9.2.1, D).

No caso de alteração de funções e/ou de mobilidade organizacional, a informação referente ao colaborador deve ser atualizada ([19], 9.2.2, E). Em caso de saída da organização, prolongada ou definitiva, por parte de um colaborador, o seu respetivo identificador único deverá ser imediatamente removido ou desativado (caso seja necessário manter a informação do utilizador e/ou *logs* de acessos) ([19], 9.2.1, B). Deve ser realizada uma revisão periódica aos utilizadores redundantes e/ou desativados ([19], 9.2.1, C).

As contas de utilizadores externos são definidas com um período de validade de acordo com o período do contrato estabelecido. De forma a facilitar a sua distinção, o respetivo identificador único de conta poderá integrar a sigla da empresa externa correspondente. A extensão de acessos atribuídos a utilizadores externos tem de ser solicitada pelo gestor de projeto, um mês antes da expiração do período de validade dos mesmos.

Atribuição e alteração de acessos Os acessos aos sistemas e aplicações são atribuídos aos utilizadores, considerando as necessidades efetivas para o desempenho das suas funções, com base no princípio *least privilige* e *need to know* (2.4.2).

Os pedidos de acesso devem ser únicos e adaptados às necessidades do colaborador. Replicações de pedidos submetidos anteriormente por outros colaboradores ou pedidos que têm por base acessos de outros utilizadores devem ser evitados.

Para cada aplicação, tem de existir pelo menos um responsável por aprovar pedidos de acesso, mudanças de perfis e permissões, sendo que nenhum indivíduo pode ter os privilégios necessários para aprovar os seus próprios pedidos de acesso.

O princípio da segregação de funções deve ser cumprido, sendo qualquer exceção a este alvo de análise, registo e aprovação. Em caso de aprovação, é necessária a definição de controlos mitigatórios.

Deve de ser mantido um registo central de acessos e privilégios concedidos aos utilizadores ([19], 9.2.2, D) e estes só podem ser efetivamente atribuídos, após os procedimentos de aprovação estarem concluídos e formalmente registados ([19], 9.2.2, D).

A alteração de acessos atribuídos é efetuada sempre que:

- Seja aprovado um pedido de alteração de acessos;
- Ocorram mudanças na estrutura orgânica da organização;
- Sejam alteradas as funções do colaborador;
- No âmbito da revisão periódica de utilizadores ativos nos sistemas e respetivos acessos sejam detetadas não-conformidades.

Desativação de acessos A desativação de acessos atribuídos a um participante consiste na colocação da sua conta de acesso num estado que impede o acesso aos sistemas de informação. A desativação de acessos atribuídos a um participante é efetuada sempre que:

- O colaborador encerre as suas funções na organização ([19], 9.2.6, A);
- Exista uma ausência de serviço prolongada por parte do participante (ex: situações de baixa por doença, serviços recorrentes de prestadores de serviço);
- O superior hierárquico do colaborador o solicite;
- A conta não seja utilizada há mais de 60 dias;
- Tenha terminado o período de validade atribuído à conta;
- No âmbito da revisão periódica de utilizadores ativos nos sistemas e respetivos acessos sejam detetadas não-conformidades.

6.4 Processos

Os processos de gestão de identidades e acessos foram desenhados de acordo com o ciclo de vida dos utilizadores, estando os mesmos em linha com as diretrizes e controlos que constam na norma de gestão de identidades e acessos (6.3.2).

A definição de processos apresenta benefícios como o aumento de eficiência, a transparência dos acessos, a mitigação de riscos de acessos indevidos e a gestão eficiente e efetiva dos acessos de todos os colaboradores.

Na figura 6.10, podemos observar os processos responsáveis pela gestão do ciclo de vida dos utilizadores, de 1 a 4, e os processos auxiliares A e B, responsáveis pela gestão de perfis e monitorização, respetivamente.

Todos os processos foram construídos de forma generalizada e sem recorrer a uma ferramenta de gestão de identidades e acessos específica, de modo a tornar possível o ajuste dos mesmos aos diferentes ambientes e sistemas existentes nas organizações.

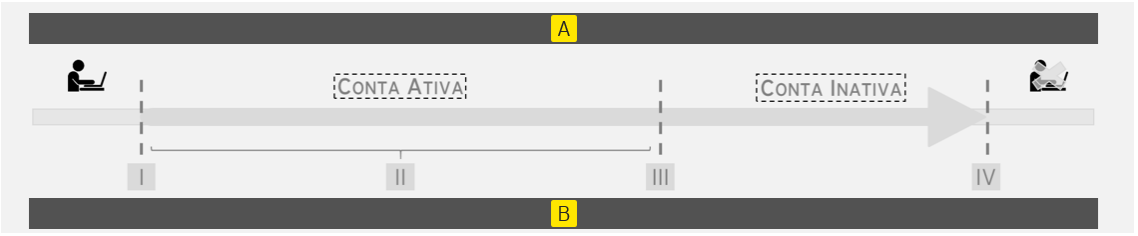

Figura 6.10: Processos do ciclo de vida do utilizador

6.4.1 Processo de gestão de perfis (A)

Para uma gestão e administração eficaz dos acessos aos vários sistemas e aplicações, deve ser definido um processo de gestão de perfis que permita mitigar situações de risco *à priori*, promovendo a homogeneização de acessos dentro da mesma função na organização. O processo definido está alavancado na criação de pacotes de acessos e permissões, desenhados por função organizacional.

- **Sub-processo GP1: Criação e alteração de perfis funcionais**

  Sub-processo responsável pela construção ou alteração dos perfis funcionais. A atribuição de acessos e permissões aos utilizadores é realizada através da concessão desses perfis. Um perfil funcional contém todos os acessos e permissões necessárias para o utilizador desempenhar as suas funções.

  A necessidade de criação ou alteração de perfis é identificada por um dos *key users* funcionais. Este identifica riscos inerentes à combinação de acessos e permissões, propondo controlos mitigatórios se necessário.

O gestor de risco aprova os riscos e controlos propostos e, de seguida, o diretor de 1ª linha aprova ou reprova o perfil funcional, de acordo com os riscos e controlos identificados.

Após a aprovação, o repositório de perfis é atualizado e os privilégios são alterados no respetivo repositório, quando aplicável.

- **Sub-processo GP2: Criação e alteração de perfis aplicacionais**

  Sub-processo responsável pela construção ou alteração de perfis nas aplicações. O perfil aplicacional agrega as permissões que os utilizadores podem deter ao nível da aplicação.

  A necessidade de criação ou alteração de perfis é identificada e comunicada pelo *key user* funcional à equipa de administração e/ou equipa de desenvolvimento, que avaliam a possibilidade técnica de criação/alteração de perfil.

  Caso se verifique a possibilidade, é efetuada uma análise de risco inerente às permissões, propondo controlos mitigatórios, se necessário.

  Tal como no sub-processo GP1, o gestor de risco aprova os riscos e controlos propostos e, de seguida, o diretor de 1ª linha aprova o perfil aplicacional, de acordo com os riscos e controlos identificados.

  Após a aprovação, o repositório de perfis é atualizado e as permissões são alteradas, quando aplicável.

- **Sub-processo GP3: Revisão de perfis**

  A revisão é realizada periodicamente de forma a garantir adequação dos perfis existentes. O *key user* funcional é responsável por analisar a lista de forma a perceber se existem perfis desatualizados ou inadequados face às funções existentes.

  Caso ocorram inconformidades, dá-se inicio ao processo de remoção ou alteração de perfil funcional e/ou aplicacional.

- **Sub-processo GP4: Remoção de perfil funcional**

  A remoção de perfis surge do desalinhamento de perfis, face à realidade organizacional. O processo de remoção de perfis funcionais pode surgir do processo de revisão dos mesmos ou através de um pedido de remoção explícito.

  A remoção do perfil está sujeita à aprovação do diretor de 1ª linha.

  Após aprovação, o perfil é retirado do repositório e todos os acessos associados são removidos.

- **Sub-processo GP5: Remoção de perfil aplicacional**

O processo de remoção de perfil aplicacional é constituído pelos mesmos passos presentes no sub-processo anterior, GP4. Neste tipo de remoção é também necessário validar se existe algum impedimento técnico nos sistemas, antes de proceder à análise de risco.

6.4.2 Processo de *onboarding* (I)

Processo de integração de novos colaboradores nos sistemas de informação da organização. Este despoleta a criação de uma identidade e a atribuição de acessos e permissões, permitindo aos utilizadores desempenhar rapidamente as suas funções.

Este inicia-se com a introdução dos atributos do utilizador no sistema de recursos humanos. Com base nessa informação, serão criadas as suas credenciais e atribuído o respetivo perfil pré-aprovado com base na sua função e/ou área em que irá ingressar.

Em caso de necessidade de acessos privilegiados, estes terão de ser aprovados pelo diretor de primeira linha correspondente.

6.4.3 Processo de alteração (II)

Processo de alteração de uma identidade e respetivos acessos e permissões, despoletado por uma mudança de funções, área e/ou empresa dentro da organização. O processo de acessos de emergência será despoletado em caso de necessidade de acesso pontual.

- **Sub-processo AL1: Mobilidade funcional**

  O sub-processo inicia-se aquando de uma mudança organizacional (ex.: alteração de funções, área e/ou empresa). Os atributos do utilizador são alterados no sistema e o seu perfil anterior é removido, bem como todos os acessos e permissões associados ao mesmo.

  Após a remoção, um novo perfil será atribuído tendo em conta a nova função.

  Em caso de necessidade de acessos privilegiados, estes terão de ser aprovados pelo diretor de primeira linha correspondente.

- **Sub-processo AL2: Acessos de emergência**

  Os acessos de emergência correspondem a acessos atribuídos temporariamente em situações de necessidade repentina. Estes poderão corresponder a acessos privilegiados, dependendo da constituição dos mesmos.

  A atribuição destes acessos é realizada sem recorrer a perfis existentes e terá de ser aprovado pela diretor de primeira linha.

  Após a sua utilização, os acessos são removidos e as tarefas/atividades realizadas são analisadas.

6.4.4 Processo de desativação e reativação de conta (III)

Processo de desativação da conta do utilizador, em consequência da alteração do seu estado laboral ou desatualização das credenciais. A reativação da conta e o *reset* de *passwords* permite ao utilizador voltar a usufruir dos acessos e permissões que detinha.

- **Sub-processo DR1: Desativação do utilizador**

  A desativação de credenciais pode ter origem numa alteração de estado do utilizador (ex: licença de maternidade ou baixa médica) ou numa expiração de validade de conta e/ou *password*.

  Quando um utilizador não se encontra a representar as suas funções ou quando é atingido o fim do período de validade da sua conta (ex: término de serviços externos) esta deverá ser desativada tanto nas aplicações a que o utilizadores tem acesso como no serviço de diretoria (ex: Active Directory), quando aplicável.

- **Sub-processo DR2: Reativação do utilizador**

  A reativação do utilizador acontece em situações de extensão de um contrato laboral ou reativação de funções após período de ausência.

  O sub-processo inicia com a alteração dos atributos do utilizador, seguido da reativação da sua conta de acesso ao domínio e dos respectivos acessos às aplicações que constituem o seu perfil funcional.

  Fruto da reativação de conta, a *password* deve também ser alterada no primeiro acesso.

- **Sub-processo DR3: Reset de *password***

  A solicitação de reset de *password* pode derivar de vários motivos como: esquecimento ou bloqueio de credenciais (fruto de tentativas excessivas de l*ogin*).

  De forma a reaver as suas credenciais de acesso, o utilizador deve validar a sua identidade através do método definido pela organização.

  Após a validação, deve ser lhe entregue uma nova *password default*, que deverá ser alterada no primeiro *login*/acesso realizado.

6.4.5 Processo de *offboarding* (IV)

Processo relativo à saída de um colaborador da organização. A definição deste processo permite garantir a remoção de utilizadores que já não precisam de ter acessos.

O processo inicia com a alteração dos atributos do utilizador, seguido da desativação da sua conta de acesso ao domínio e remoção de todos acessos às aplicações e permissões que constituem o seu perfil funcional.

A conta de domínio poderá também ser removida completamente, dependo da política de armazenamento de *logs* definida pela organização.

6.4.6 Processo de monitorização (B)

O processo de monitorização é sustentado em processos periódicos de revisão de identidades e acessos. Estes processos permitem à organização apresentar um maior controlo e segurança, através da identificação de exceções, análise de *logs* considerados críticos para a organização e riscos de acessos e permissões atribuídos.

- **Sub-processo MO1: Revisão de identidades**

  Periodicamente, a equipa de administração de sistemas é responsável por extrair a lista de utilizadores e fazer chegar essa informação aos *key users* funcionais existentes na organização.

  Caso sejam identificados utilizadores indevidos ou atributos que contenham informação errada ou desatualizada, é da responsabilidade do gestor de identidades resolver as anomalias encontradas.

- **Sub-processo MO2: Revisão de privilégios**

  O sub-processo de revisão de acessos inicia-se com a extração de lista de perfis atribuídos a cada utilizador no repositório de privilégios e da lista de acessos e permissões atribuídos em cada uma aplicações.

  É da responsabilidade de cada um dos *key users* funcionais, analisar os acessos atribuídos e perceber que estes se encontram sincronizados com o repositório de privilégios.

  Caso sejam encontradas anomalias, as mesmas devem ser notificadas aos responsáveis pelo utilizador e à administração de sistemas para que possam ser corrigidas.

Capítulo 7

Fase 3 - Definição do roadmap de implementação

Neste capítulo será apresentado o conjunto de iniciativas acionáveis, que poderão ser implementadas no decorrer da fase 4 (fase de implementação).

As iniciativas são definidas tendo em conta as duas primeiras fases do programa: diagnóstico, que visa aferir a maturidade da organização, nomeadamente existência de políticas, processos e tecnologias e; definição do modelo futuro, onde é definido o modelo de governo, normas de apoio, e processos *end-to-end*.

Estas permitem endereçar as oportunidades de melhoria identificadas ao longo dos vários domínios e visam dotar a organização das ferramentas e recursos necessários para implementação do modelo definido.

O programa contempla iniciativas core, representadas na figura 7.1 pelos números 1,2 e 3, e duas iniciativas extra referentes à aquisição de uma ferramenta automática de gestão de identidades e acessos, representadas pelos números 4 e 5. O objetivo das mesmas encontram-se descrito abaixo.

Figura 7.1: Iniciativas que constituem o *roadmap* de implementação

- **Definição de perfis, riscos e controlos:** Definir os perfis funcionais que servirão de base ao modelo de gestão de identidades e acessos, suportados em análises de risco e definição de controlos mitigatórios.

- **Revisão de controlo de acessos das aplicações:** Rever os utilizadores, acessos e permissões nas aplicações a incluir no modelo, de forma a refletir as normas e análise funcional efetuada em sistema.

- **Seleção e implementação das tecnologias de suporte:** Selecionar e implementar a tecnologia(s) de suporte à gestão de identidades e acessos, permitindo automatizar processos definidos.

- **Integração de aplicações:** Integrar aplicações abrangidas pelos perfis funcionais definidos na tecnologia de suporte e cujos acessos tenham sido previamente revistos de forma a refletir a análise realizada junto das áreas.

- **Implementação do modelo definido:** Implementar modelo de governo, processos de gestão de identidades e acessos e normas de suporte ao modelo de de gestão de identidades e acessos.

Tendo em conta que o presente *roadmap* apresenta como principal objetivo ajudar pequenas e médias empresas a implementar e gerir o seu próprio modelo de identidades e acessos e, dado que, estas empresas, por norma, não dispõem de capital disponível para este tipo de investimento, a implementação das iniciativas 4 e 5 não será considerada obrigatória para o sucesso do mesmo.

7.1 Fatores criticos de sucesso

São vários os fatores considerados críticos para o sucesso da implementação do modelo de gestão de identidades e acessos, entre eles podemos destacar:

Cultura Para um programa bem-sucedido, a cultura da organização precisa de ser adaptada para que os participantes compreendam a importância do papel que desempenham no modelo de governo e na execução dos processos de gestão de identidades e acessos.

Liderança A liderança do programa deve ter poder, influência, visibilidade e experiência no assunto para gerar mudança.

Compromisso O compromisso das partes interessadas no programa é fundamental, impulsionado pela comunicação de sucesso de forma a ajudar os outros a aceitar ou adotar o programa.

Comunicação A estratégia de comunicação deve focar-se em comunicar de forma clara a visão do programa. A visão deve ser anunciada, com conteúdo informativo sobre a iniciativa de forma a incentivar os colaboradores a envolverem-se em atividades futuras.

Capacitação Capacitar os funcionários, desenvolvendo o conhecimento necessário para gerir e responder às mudanças introduzidas pelo programa. Os níveis de competências vão desde o treino básico até o domínio de processos de gestão de identidades e acessos, novos ou modificados.

7.2 Metodologia de implementação

Devido à complexidade e dimensão do portfólio por vezes encontrado, o programa deve começar por um piloto, seguido de várias fases de implementação, de forma a diminuir possíveis constrangimentos no negócio ao longo da implementação. A definição de perfis funcionais e posterior integração de aplicações no modelo, deve ser efetuada por direção, ao longo das várias waves.

A definição de waves por direção, em detrimento da definição por aplicação, irá trazer vantagens como:

- Menor risco de interrupção de negócio;
- Transição mais sustentada, com maior maior tempo de prepação e de ajuste;
- Ganhos e resultados imediatos para a organização;
- Diminuição da complexidade de integração ao longo do programa;
- Minimização do esforço associado à criação da matriz de segregação de funções.

Contudo, poderá trazer desvantagens como a existência de aplicações com processos de gestão de acessos paralelos, durante a fase de transição e uma maior concentração de esforço por área.

7.3 Definição de perfis, risco e controlos (I)

Iniciativa responsável pela definição dos perfis funcionais que servirão de base ao modelo, suportados em análises de risco e definição de controlos mitigatórios.

A. Levantar características e necessidades do negócio

- Identificar áreas e funções existentes na organização;
- Identificar aplicações utilizadas e atividades desenvolvidas;
- Analisar as responsabilidades, intervenção em processos e respetivas atividades de cada função dentro da organização;
- Identificar *key users* funcionais e responsáveis pela aprovação de matriz de acesso (diretores de primeira linha e gestão de risco).

B. Definir/atualizar riscos de TI e controlos

- Definir riscos e respetivo impacto e criticidade relacionados com a gestão de acessos, designadamente acesso indevido à informação, alteração de informação não autorizada, fraude ou acesso indevido a componentes chave do ambiente produtivo e da rede com impacto na atividade da organização;
- Definir controlos preventivos, detetivos e/ou corretivos para riscos identificados no ponto anterior. Os controlos poderão ser automatizados, manuais ou parcialmente automatizados.

C. Definir matriz de riscos de segregação de funções

- Identificar funções críticas do negócio e suporte ao negócio (acessos sensíveis) por direção e mapear com permissões em sistema;
- Desenvolver matriz de combinações tóxicas aplicável a todos os processos e aplicações.

D. Definir perfis funcionais, por direção (em linha com o encadeamento definido por wave):

- Definir nomenclatura de perfis funcionais, perfis aplicacionais, permissões e descrições *business friendly* para todos os campos;
- Definir perfil funcional por função existente em cada direção e perfis privilegiados, detalhando que aplicações serão incluídas no perfil funcional e qual o conjunto de perfis aplicacionais associados. A constituição do perfil funcional encontra-se descrita na figura 7.2;

- Identificar riscos por perfil funcional;
- Remediar os conflitos identificados nas análises de risco: remoção de acesso conflituante ou definição de controlo mitigatório.

A definição de perfis funcionais e aplicacionais é influenciada por dois fatores: existência de perfis de acesso na aplicação e granularidade de permissões suportada pela aplicação. Os seguintes aspetos deverão ser tidos em consideração aquando da definição:

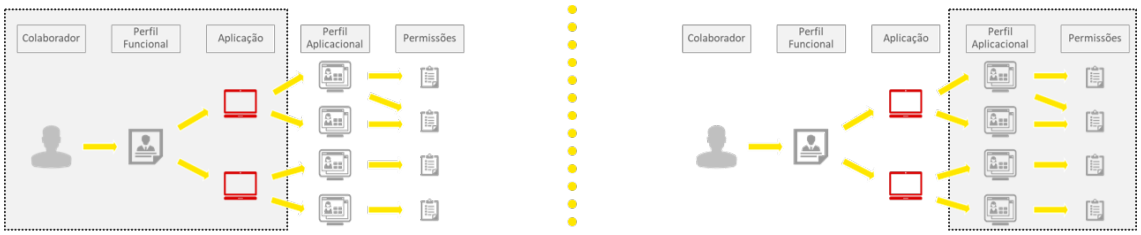

Figura 7.2: Constituição do perfil funcional

- **Aplicações sem perfil de acesso**: se tecnicamente viável, desenvolver interface para controlo de acessos. Caso não seja, e de acordo com risco existente, definir controlo mitigatório.
- **Aplicações com perfil de acesso à base de dados**: se tecnicamente viável, o acesso por parte do negócio deverá ser feito via perfil de acesso aplicacional, o acesso direto a tabelas e *views* deve ser evitado.
- **Aplicação com perfil de acesso aplicacional, segregado por acesso a transações e objetos**: definir transações e objetos por função.
- **Aplicação com perfil de acesso aplicacional, segregado por acesso a menus e/ou janelas**: se tecnicamente viável, desagregar os menus de acordo com a menor granularidade permitida pela aplicação. Identificar atividades embebidas em cada menu de acessos, e contemplar a agregação de atividades aquando da definição de perfis.

Nota: A definição de acessos por perfil funcional poderá ser acompanhada por uma análise de custos de licenciamento, com vista a otimizar a utilização das mesmas por utilizador e função.

E. Definir acessos de emergência: os mesmos deverão ter as permissões mínimas essenciais, em detrimento de acessos alargado.

7.4 Revisão do controlo de acessos (II)

Iniciativa responsável pela revisão dos utilizadores, acessos e permissões nas aplicações a incluir no modelo, de forma a refletir em sistema, as normas e análise funcional efetuada.

A. Rever permissões nas aplicações

- Configurar permissões de acordo com a definição funcional (iniciativa 2: Definição de perfis funcionais, riscos e controlos);
- Transportar configuração para ambiente de testes;
- Preparar e executar testes unitários e de aceitação;
- Transportar configuração para ambiente de qualidade/produção.

B. Rever contas de utilizador presentes em cada aplicação

- Definir nomenclatura de utilizadores, em linha com a norma de gestão de identidades e acessos;
- Rever utilizadores tendo em consideração os acessos definidos por função;
- Identificar contas de serviço e contas com acessos privilegiados.

C. Parametrizações adicionais

- Ativar ou desenvolver, sempre que tecnicamente viável, manutenção de *logs* de acesso e de execução de atividades críticas;
- Ativar ou desenvolver parametrização para inativação de utilizadores após a expiração da validade dos privilégios atribuído.

D. Limpeza do serviço de diretoria

- Rever domínios e grupos criados no serviço;
- Remover objetos não utilizados (grupos, máquinas inativas, *fileshares*, listas de distribuição);
- Identificar e remover grupos cíclicos ou duplicados;
- Remover contas inativas;
- Identificar e remover contas temporárias para fins de testes;
- Popular atributos mandatários de utilizadores sempre que possível.

E. Consolidação com serviço de diretoria

- Definir requisitos de modo a que a autenticação, na maioria das aplicações, seja realizada através da conta de domínio. Este tipo de autenticação pode ser conseguido, por exemplo, através do uso do protocolo LDAP, em arquiteturas *on-prem* ou através do protocolo *SAML* em arquiteturas baseadas em *cloud*. A lista de protocolos existentes pode ser consultada na secção 2.3.3;
- Desenvolver plano de implementação da funcionalidade;
- Desenvolver e testar alterações.

F. Definir repositório de privilégios Definir um repositório de privilégios que contemple informação sobre todos os utilizadores e respetivo perfil funcional, de forma a obter visibilidade sobre os privilégios atribuídos em todos os sistemas e aplicações (sincronizados ou não com o serviço de diretoria).

7.5 Implementação do modelo definido (III)

Implementar modelo de governo, processos de gestão de identidades e acessos, e normas de suporte ao modelo de gestão de identidades e acessos.

A. Implementação do modelo de governo

- Definir a estrutura de reporte e articulação entre os diferentes atores do modelo de governo e restante organização;
- Nomear comités e equipas;
- Definir a estratégia de transição entre modelos;
- Divulgar missão e objetivos do programa em localização acessível por todos os colaboradores;
- Publicar modelo de governo, em localização acessível por todos os colaboradores.

É aconselhado que os membros de cada equipa possuam um conjunto de características e conhecimentos transversais para o desempenho das suas funções, em particular:

- Comité Executivo
  - Competências para tomada de decisão;
  - Capacidade de fornecer orientações estratégicas;
  - Capacidade de definir as expectativas e as medidas de sucesso;
  - Capacidade de resolver conflitos de natureza estratégica e organizacional.
- Comité de Governance
  - Competências em análise de risco;
  - Capacidade de comunicar de forma clara e transparente com todas as partes envolvidas;
  - Conhecimento sobre as necessidades da organização ao nível dos sistemas;
  - Capacidade de análise em relação à viabilidade e eficiência dos aspetos relevantes;
  - Conhecimento abrangente do setor e dos processos da organização.
- Equipa de Identidades
  - Conhecimento das necessidades de negócio em termos da utilização de sistemas e aplicações;
  - Conhecimento das boas práticas de gestão de identidade;

  - Conhecimento das políticas definidas na organização;
  - Conhecimento/visibilidade do estado laboral dos utilizadores (por tipo de utilizador);
  - Competências para a administração dos sistemas de gestão de identidades.

- Equipa de Acessos
  - Capacidade de analisar requisitos aplicacionais e definir processos;
  - Conhecimento sobre os processos de aprovisionamento e desaprovisionamento;
  - Conhecimento das permissões existentes nos sistemas e aplicações;
  - Conhecimento/visibilidade dos acessos, permissões, riscos e controlos atribuídos aos utilizadores.

- Equipa de Monitorização
  - Conhecimento de boas práticas de gestão de identidades e acessos;
  - Conhecimento de metodologias de monitorização de processos;
  - Conhecimento sobre as políticas em vigor na organização;
  - Conhecimento dos riscos inerentes à gestão de identidades e acessos;
  - Capacidade de análise da informação recolhida.

- Equipa de Gestão de Perfis
  - Conhecimento de boas práticas de gestão de perfis;
  - Conhecimento dos riscos inerentes à gestão de identidades e acessos;
  - Conhecimento para a definição de controlos para a mitigação de riscos;
  - Conhecimentos técnicos sobre os sistemas e aplicações.

B. Implementar normas

- Publicar norma de gestão de identidades e acessos e norma de *passwords* em localização acessível por todos os colaboradores;
- Definir um processo periódico de revisão de adequação de normas;
- Reforçar o cumprimento das normas aprovadas, sempre que tecnicamente viável, nomeadamente através de controlos que se referem a mecanismos de autenticação, e respetivos parâmetros (ex: *passwords*);
- Definir uma *baseline* de segurança de informação com base na norma de gestão de acessos e passwords, a ter em consideração aquando da seleção de um sistema/aplicação.

C. Selecionar/adequar aplicações de suporte à gestão de identidades

- Selecionar aplicação de suporte à gestão de identidades de externos, devendo a mesma garantir:
  - A manutenção dos atributos necessários por identidade: nome, empresa, direção responsável pelo projeto, data de início e fim de projeto;
  - A obrigatoriedade de preenchimento dos atributos mandatários;
  - A sincronização com o serviço de diretoria para atualização dos atributos.
- Adequar aplicações de suporte à gestão de identidades de internos e temporários, devendo a mesma garantir:
  - A manutenção dos atributos necessários por identidade: nome, empresa, direção onde colaborador está alocado, função, data de início e fim de contrato;
  - A obrigatoriedade de preenchimento dos atributos mandatários;
  - A ligação com o serviço de diretoria para atualização dos atributos.

F. Implementar processos

- Definir formulários e templates de apoio aos processos definidos
  - Gestão de perfis
    - Formulário de criação/alteração de perfis funcionais – ID do pedido, ID do requester, explicação da necessidade, identificação do grupo de utilizadores a que o perfil se destina, das aplicações, das permissões, dos riscos e controlos (caso existam);
    - Relatório de aprovação de riscos e controlos – ID do pedido, ID do aprovador, decisão e explicação, identifica controlos adicionais (caso necessário);
    - Formulário de descrição do controlo mitigatório – ID do pedido, ID do requester, descrição do controlo, método de aplicação do controlo;
    - Formulário de alteração de criação/alteração de perfis aplicacionais – ID do pedido, ID do requester, explicação da necessidade, identificação da aplicação e das permissões;
    - Relatório com viabilidade e estimativa de esforço – ID do pedido, ID do avaliador, descrição da análise realizada aos requisitos;
    - Relatório com os riscos identificados – ID do pedido, ID do avaliador, identificação de riscos (caso existam);
    - Descrição do controlo mitigatório (em anexo ao relatório anterior) – ID do pedido, ID avaliador, identificação de controlo;

  - Lista de acessos e permissões – ID de revisão de perfis, listagem de perfis, acessos e permissões associados, número de atribuições, direções atribuídas;
  - Formulário de alteração de remoção de perfil funcional - ID do pedido, ID do requester, explicação da necessidade, identificação do grupo de utilizadores afetados, das aplicações, das permissões;
  - Formulário de alteração de remoção de perfis aplicacional - ID do pedido, ID do requester, explicação da necessidade, identificação da aplicação e das permissões.

- Gestão do ciclo de vida do utilizador
  - Formulário de pedido de acesso emergências – ID do pedido, ID do requester, aplicação, acessos pretendidos, razão do acesso;
  - Relatório de aprovação de acesso de emergência – ID do aprovador, decisão e explicação;
  - Registo de logs – ID do utilizador, logs das atividades desenvolvidas pelo utilizador;
  - Relatório de atividades de acessos de emergência – ID avaliador, ID do utilizador, resultados da análise dos logs das atividades, definição de medidas de ação (caso tenha sido identificado anomalias nos logs.

- Monitorização
  - Lista de utilizadores – ID de revisão de identidades, lista de utilizadores, atributos do utilizador;
  - Relatório com a lista de atualizações de identidades – ID de revisão de identidades, ID de avaliador, descrição de anomalias, identificar ações a desenvolver;
  - Lista de acessos e permissões (repositório) - ID de revisão de identidades, lista de utilizadores, de perfis, de acessos e permissões associados;
  - Lista de acessos e permissões (aplicações) - ID de revisão de identidades, identificação da aplicação, lista de utilizadores e permissões atribuídas;
  - Relatório com exceções - ID de revisão de identidades, identificação de anomalias e ações a desenvolver (caso existam);
  - Lista de logs de acessos – ID de revisão de logs, identificação da aplicação, registos de logs por utilizadores, autorizações atribuídas;
  - Relatório com exceções - ID de revisão de logs, identificação de anomalias e ações a desenvolver (caso existam).

7.6 Seleção e implementação de tecnologia de suporte (IV)

Selecionar e implementar a tecnologia(s) de suporte à gestão de identidades e acessos, permitindo automatizar processos definidos.

A escolha de tecnologia(s) envolve uma ponderação custo-benefício que poderá estar alavancada na priorização dos seguintes critérios: pontos críticos que conseguem ser endereçados, cobertura do risco, impacto no processo de gestão de identidades e acessos, complexidade de implementação e custo de implementação.

A. Selecionar tecnologia(s) de suporte

- Confirmar aplicações para integração na ferramenta;
- Definir o modelo de avaliação de propostas, considerando os atributos de avaliação, respetivos ponderadores e escalas de avaliação;
- Preparar o caderno de encargos com base na definição de requisitos técnicos e funcionais;
- Lançar RFP (*Request for proposal*) formal de consulta ao mercado;
- Sistematizar e analisar resultados da avaliação de fornecedores;
- Negociar e selecionar fornecedor.

B. Implementar ferramenta(s) e tecnologia(s) de suporte

- Desenhar a solução técnica da ferramenta (arquitetura, modelo de dados, integrações);
- Definir casos de uso e desenhar o plano de testes;
- Instalar e configurar a ferramenta nos vários ambientes;
- Integrar com sistemas e desenvolver as integrações necessárias;
- Executar o plano de testes (unitários, integração e aceitação);
- Efetuar a passagem a produção da solução;
- Suportar a utilização dos novos sistemas após entrada em produção.

7.7 Integração de aplicações em tecnologia de suporte (V)

Integrar aplicações abrangidas pelos perfis funcionais definidos e cujos acessos tenham sido previamente revistos, de forma a alavancar o modelo definido.

A. Integração das aplicações

- Integrar dados da aplicação;
- Parametrizar ligação entre tecnologia e a aplicação alvo;
- Desenvolver *APIs* para permitir chamada pela tecnologia, se necessário;
- Desativar funcionalidades na aplicação que passarão a ser geridas pela ferramenta (ex: gestão de perfis, gestão de utilizadores, gestão de passwords);
- Definir e testar casos de uso;
- Suportar a utilização dos novos sistemas após entrada em produção.

Capítulo 8

Validação do modelo

De forma a validar a metodologia definida e respetivo modelo resultante, será apresentado o nível de maturidade esperado, após implementação. Serão também descritos os principais benefícios do mesmo e de que forma serão proporcionados.

8.1 Nível de maturidade alcançado

Na presente secção, podemos observar os níveis de maturidade esperados em cada domínio, após implementação das iniciativas *core* (capítulo 7, I a III) numa organização.

Cada sub-domínio foi avaliado, através da atribuição de um nível de maturidade de 1 a 5. O significado geral de cada nível pode ser consultado na figura 8.1, podendo ocorrer algumas excepções (descritas no sub-domínio correspondente).

Figura 8.1: Significado dos níveis de maturidade

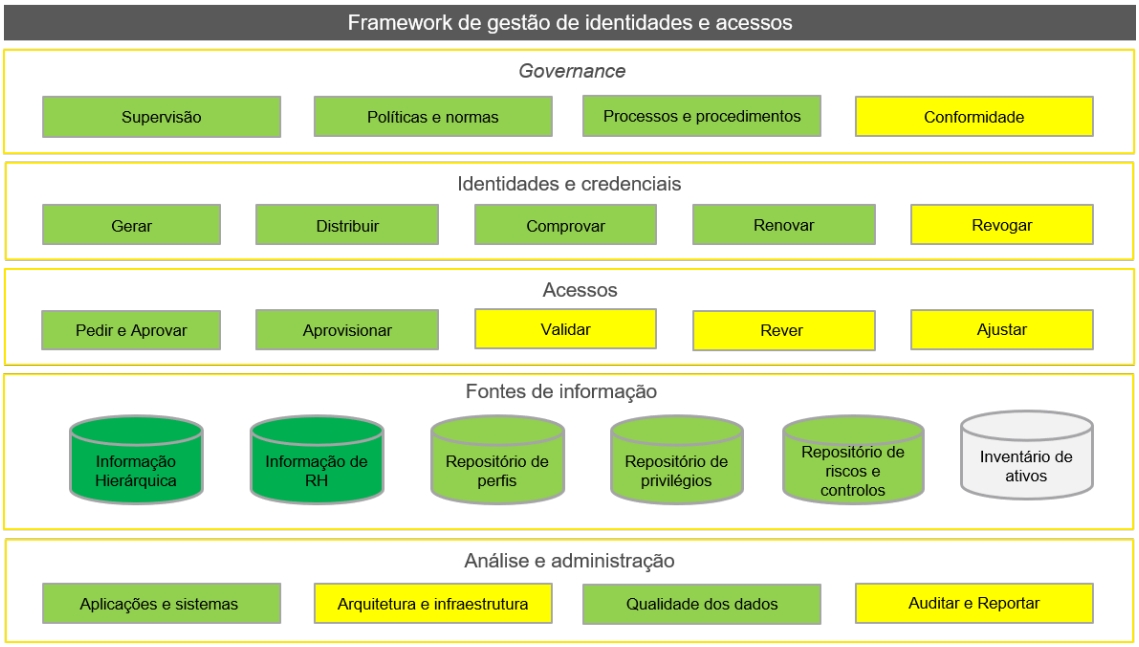

Figura 8.2: Estado de maturidade alcançado

Governance

- Supervisão (Nível 4): aplicando o modelo de governo, proposto em 6.2, todas as responsabilidades referentes à gestão de identidades e acessos irão passar a estar completamente definidas, facilitando o processo de supervisão. Para atingir o nível 5 é necessário que os responsáveis máximos da organização, participem diretamente na gestão e supervisão do programa.

- Politicas e normas (Nível 4): utilizando como referência, os controlos descritos em 6.3.1 e 6.3.2, na definição das normas para *password* e de gestão de identidades e acessos, respetivamente, a organização atingirá o nível 3 de maturidade. Assim que estas se encontrem publicadas e aplicadas a toda a organização, será atingido o nível 4. Esta poderá atingir o nível 5, se a revisão das normas definidas for efetuada de forma periódica e sempre que surjam novas regulamentações ou iniciativas de negócio.

- Processos e procedimentos (Nível 4): tendo como exemplo os processos definidos em 6.4 , o grupo poderá alcançar o nível 4 de maturidade. Os processos definidos cobrem todo o ciclo de vida do utilizador dentro da organização, existindo ainda processos de suporte à monotorização e à criação / gestão de perfis. O nível 5 poderá ser alcançado quando todos os processos passarem a ser automatizados, garantindo o cumprimento dos mesmos.

- Conformidade (Nível 3): aquando da publicação das normas e implementação dos novos processos definidos, a organização passará a considerar a análise de risco

e definição de controlos mitigatórios como prioridade, alcançando o nível 3 de maturidade.

Identidades e credenciais

- Gerar (Nível 4): através da promoção do uso de identificador global único para cada utilizador e da criação de *password* fortes em todas as credenciais, a organização atingirá o nível 4 de maturidade. O nível 5 só pode ser alcançado com uma ferramenta de gestão de identidades e acessos que faça a correlação de forma automática, entre a identidade e as várias credenciais que poderão estar associadas a esta.

- Distribuir (Nível 4): aquando da definição do modelo de governo e respetivas responsabilidades, a processo de distribuição de credenciais passará a ser uniforme ao longo de toda a organização. As credenciais globais de acesso poderão ser comunicadas à chefia, por exemplo, enquanto que outras credenciais, se necessárias, poderão posteriormente ser comunicadas por e-mail. A password deverá ser alterado na primeira utilização.

- Comprovar (Nível 4): o método de comprovação de identidade será descrito durante a definição da norma para *passwords* (6.3.1) e do processo de *reset* de *password* (6.4.4, DR3). Os níveis 4 e 5, serão alcançados assim que o método seja aplicado a todas aplicações e sistemas da organização e quando essa comprovação for realizada através de sistema, respetivamente.

- Renovar (Nível 4): a implementação do processo de reativação (6.4.4, DR2), assegura a reativação e/ou renovação das credenciais do utilizador. Nos casos em que as credenciais tem de ser repostas, o processo de *reset* (6.4.4, DR3), descreve todo o procedimento necessário para o realizar. O nível 5 pode ser alcançado automatizando estes processos, recorrendo a uma plataforma de *self-service*.

- Revogar (Nível 3): a revogação de credenciais é fruto do processo de revisão de identidades (6.4.6, MO1). Dada a natureza manual e por vezes falível do mesmo, não poderá ser alcançado um nível superior de maturidade.

Acessos

- Pedir e aprovar (Nível 4): na definição e implementação de todos os processos envolvidos na gestão de identidades e acessos, serão descritos os procedimentos relacionados com pedidos e aprovações. O nível 5 será facilmente atingido se a organização tiver ao seu alcance uma plataforma automática de *ticketing* (*ITSM*), que irá permitir uma maior rastreabilidade e sistematização dos pedidos e aprovações efetuadas, através da utilização de formulários e *templates* pré- definidos. Alguns dos possíveis formulários encontram-se descritos na secção (7.5, F).

- Aprovisionar (Nível 4): o aprovisionamento de acessos é realizado aquando da entrada do colaborador na organização. Todos os acessos necessários ao desempenho das funções do colaborador serão atribuídos a priori. O processo de onboarding (6.4.2) descreve o aprovisionamento referido. Caso seja necessário algum acesso adicional, o colaborador poderá solicitá-lo durante um tempo limitado, através do processo de alteração de acessos (6.4.3, AL2), desde que o mesmo seja aprovado.

  Um volume anormal de pedidos de acesso à mesma aplicação, partindo de colaboradores que partilhem a mesma função, poderão indicar a necessidade de revisão do perfil funcional em causa.

- Validar (Nível 3): após a implementação da iniciativa de revisão de controlo de acessos (7.4), a autenticação da maioria das aplicações existentes na organização passará a ser efetuada através da conta de domínio do colaborador, garantindo requisitos suficientes para atingir o nível 3 de maturidade. O nível 4 será atingido quando todas as aplicações utilizarem autenticação através da conta de domínio. O nível 5 poderá ser atingido assim que todas as aplicações utilizem a tecnologia *single sign-on*, referida em 2.3.3, para efetuar o controlo de acessos.

- Rever (Nível 3): a definição e implementação do processo de revisão de privilégios (6.4.6, MO2), garantirá a revisão periódica dos mesmos. Dada a natureza manual e por vezes falível do mesmo, não poderá ser alcançado um nível superior de maturidade.

- Ajustar (Nível 3): o ajuste dos perfis atribuídos será responsabilidade da equipa de administração de sistemas, contudo, dada a dependência do processo manual (6.4.6, MO2), não poderá ser alcançado um nível superior de maturidade.

Fontes de informação

- Informação Hierárquica (Nível 5): aplicando o modelo de governo, proposto em 6.2, a informação hierárquica e as respetivas responsabilidades dos membros, referentes à gestão de identidades e acessos irão passar a estar completamente definidas.

- Informação de recursos humanos (Nível 5): devido ao processo de *onboarding* (6.4.2), todas as identidades da organização e respetivos atributos, serão armazenados corretamente na plataforma de recursos humanos. Sempre que ocorram mudanças na estrutura organizacional, estes serão atualizados, de forma despoletar o processo de mobilidade funcional (6.4.3, AL1).

- Repositório de perfis e repositório de riscos e controlos (Nível 4): aquando da implementação da iniciativa de definição de perfis, risco e controlos (7.3), a organização passará a ter dois novos repositórios responsáveis pelo armazenamento de funções e respetivo perfil associado e, dos riscos e respetivos controlos mitigatórios existentes.

Dada a complexidade envolvida na gestão destes repositórios, é estimado que a organização, a curto prazo, apenas consiga atingir o nível 3 de maturidade. O nível 4 será atingido no momento em que os repositórios armazenem fielmente as funções, perfis e riscos existentes na organização.

- Repositório de privilégios (Nível 4): dada a dependência direta com repositório de perfis, o repositório de privilégios, apresentará também, o nível de 3 e 4 de maturidade, a curto e longo prazo, respetivamente.

- Inventário de ativos: o presente modelo não influencia o controlo de acessos a ativos de informação, pelo que o nível de maturidade não será influenciado.

Análise e administração

- Aplicações e sistemas (Nível 4): devido ao esforço efetuado pela organização na implementação da iniciativa de revisão do controlo de acessos das aplicações (7.4, passos A a C), será possível atingir o nível 4 de maturidade. As atividades referentes à administração de aplicações e sistemas encontram-se descritas nos processos definidos.

- Arquitetura e infraestrutura (Nível 3): devido à limpeza e consolidação do serviço de diretoria com algumas das aplicações e; à criação do novo repositório de armazenamento de informação referente aos privilégios atribuídos (7.4, D a F), a maturidade referente à arquitetura de gestão de identidades e acessos, atingirá o nível 3. O nível 4 poderá ser alcançado no momento em que todas as aplicações estejam sincronizadas com o serviço de diretoria.

- Qualidade dos dados (Nível 4): através da adoção das nomenclaturas e regras definidas na implementação da norma para *passwords* e da norma de gestão de identidades e acessos, 6.3.1 e 6.3.2, respetivamente, a qualidade dos dados será assegurada, atingindo nível 4 de maturidade.

- Auditoria e Reporte (Nível 3): a definição dos processos de revisão de identidades e privilégios, apresentados em 6.4.6, irá permitir à organização atingir o nível 3 de maturidade neste subdomínio. As melhorias passam pela definição de processos de revisão de *logs* de acessos e atividades críticas e, pela automação dos mesmos.

8.2 Exemplo de implementação do modelo

Tomando como exemplo a análise de maturidade efetuada ao estado atual da empresa X, durante a fase de diagnóstico, podemos verificar que a organização apresenta um nível médio de maturidade próximo de 2 (2.17), atingindo o patamar de parcialmente definido, como se pode observar na figura 8.1.

Aplicando o modelo de gestão de identidades e acessos definido na presente dissertação, a empresa X irá apresentar melhorias significativas, alcançando o nível médio de maturidade 3,75. Ao atingir a maturidade referida, a gestão de identidades e acessos da empresa X situar-se-á entre os patamares definido e gerido.

As diferenças entre os estados atual e futuro podem ser observadas na figura 8.3.

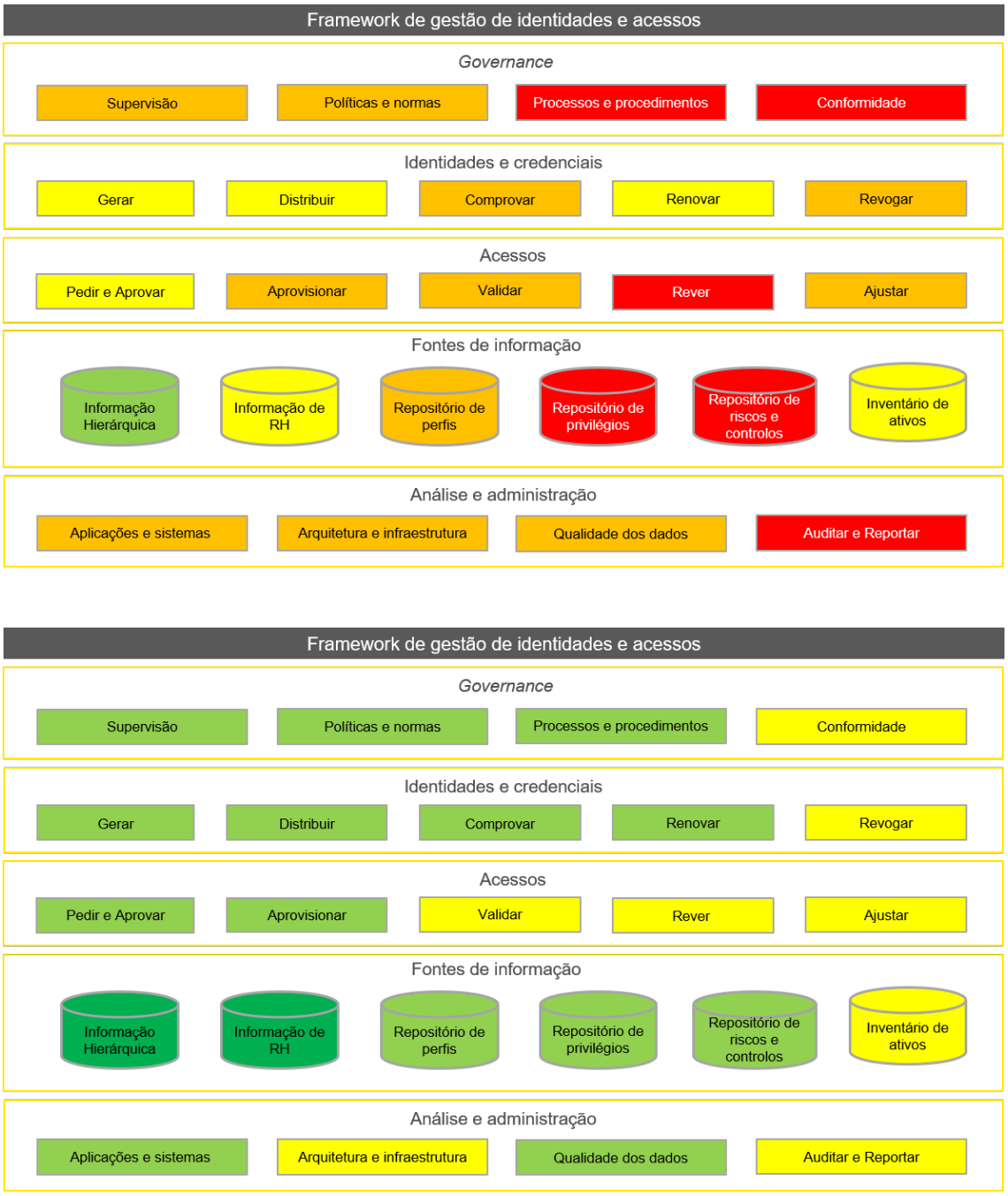

Figura 8.3: Diferenças entre o estado atual da empresa X, em cima, e o estado de maturidade possível de alcançar, em baixo

8.3 Benefícios do modelo proposto

Na presente secção, encontra-se descrito o sumário dos principais benefícios fornecidos pelo modelo de gestão de identidades e acessos definido e de que forma estes serão proporcionados.

Redução do risco e aumento de segurança

- Visão holística sobre acessos e permissões atribuídos;
- Atribuição de privilégios a funções específicas da organização, garantindo o cumprimento do principio *least privilege*;
- Limitação de situações de combinações tóxicas e acessos indevidos à informação;
- Remoção de privilégios sempre que as funções de um colaboradores são alteradas ou este deixa a organização;
- Revisão de privilégios periódica, de forma a detetar incumprimentos ou anomalias;
- Atribuição de responsabilidades, tanto na alteração de sistemas como na sua monitorização;
- Automatização de controlos e parâmetros definidos nas normas (ex: escolha de *password* forte).
- Sincronização de credenciais em diversos sistemas e aplicações. Utilizando as credenciais de domínio e mecanismos de *single sign-on*, os utilizadores não necessitam de memorizar um conjunto de credenciais, evitando o armazenamento físico das mesmas.

Aumento da produtividade

- Permite que os colaboradores sejam produtivos assim que entram na organização;
- Promove a simplificação de processos, alinhando-os com as necessidades das equipas de recursos humanos e áreas de negócio;
- Permite diminuir o tempo envolvido na aprovação de privilégios, através da atribuição de responsabilidades concretas e recorrendo a processos de atribuição definidos;
- Facilita as tarefas de administração, devido ao aumento da visibilidade sobre os privilégios atribuídos.

Melhoramento da experiencia do utilizador

- Reduz o número de credenciais existente, facilitando a sua memorização;
- Reduz as burocracias associadas com o *onboarding* e pedidos de privilégios;
- Permite diminuir o tempo envolvido na aprovação de privilégios, através da atribuição de responsabilidades concretas e recorrendo a processos de atribuição definidos;
- Reduz o esforço das equipas de administração de sistemas e suporte de TI.

Promoção da conformidade

- Promove o alinhamento para com as políticas, normas e processos definidos, facilitando processos de auditoria.

Capítulo 9

Conclusão

Na presente dissertação foram concretizados quatro objetivos principais:

- Análise e adaptação da *framework* global de gestão de identidades e acessos da EY;
- Definição da metodologia a utilizar em futuros projetos;
- Definição do modelo genérico de gestão de identidades e acessos, apresentando orientações para a definição de modelo de governo, normas e processos correspondentes;
- Definição do *roadmap* de iniciativas de apoio à implementação do modelo definido.

Em relação à análise efetuada à *framework* global de gestão de identidades e acessos da EY, foi possível identificar alguns pontos de melhoria, manifestados através da aglomeração, remoção e/ou adição de novos sub-domínios. Os passos da metodologia da EY utilizada no projeto da empresa X foram também alvo de revisão, resultando na definição de uma metodologia constituída por quatro fases distintas, com o objetivo de ser usada em projetos futuros.

Relativamente à criação do modelo genérico, a abordagem partiu da utilização da análise de maturidade atual da empresa X, identificando todas as lacunas existentes em cada um dos sub-domínios. Posteriormente, o modelo foi definido com vista a corrigir as lacunas identificadas, através da definição do modelo de governo, normas e processos, responsáveis por definir requisitos, responsabilidades e diretrizes que visam aumentar o nível de maturidade das organizações.

Quando implementado, o modelo genérico definido apresenta resultados bastantes satisfatórios. A maioria dos sub-domínios apresenta o nível 4 de maturidade, salvo algumas excepções que se encontram avaliadas num nível abaixo, devido ao carácter manual de alguns dos processos e/ou procedimentos definidos.

Melhorias adicionais ao modelo conseguido, passariam pela integração das iniciativas IV e V, resultando na aquisição e implementação de uma ferramenta de suporte, com o intuito de automatizar parte dos processos definidos. Estas iniciativas foram excluídas do *roadmap* de implementação, devido ao custo elevado que apresentam, pouco aliciante para pequenas e médias empresas.

Por fim, como exemplo prático, foi efetuada uma previsão da maturidade futura da empresa X, utilizando o modelo genérico definido. Nesta previsão, foi observada uma subida de 1.58 pontos na escala de maturidade, passando de 2.17 para 3.75, permitindo à empresa alcançar um valor muito próximo do patamar gerido (nível 4), o que demonstra a eficiência do mesmo na implementação de programas de gestão de identidades e acessos em pequenas e médias empresas.

9.1 Trabalho futuro

Como trabalho futuro, seria interessante explorar os seguintes pontos adicionais, de forma a alargar o âmbito da presente dissertação:

- Explorar as opções de ferramentas e tecnologias de gestão de identidades e acessos existentes, como é o caso das ferramentas líderes de mercado, *Sailpoint* [5] e *Okta* [7], de forma a perceber todas as suas funcionalidades e de que forma estas poderiam ser utilizadas para automatizar o modelo criado;

- Explorar as metodologias utilizadas na gestão de utilizadores e acessos privilegiados e respetivas ferramentas de apoio, como por exemplo a ferramenta líder de mercado *CyberArk* [6]. Estas ferramentas permitem efetuar um controlo exímio dos utilizadores privilegiados através da utilização de *password vaults*, do controlo e monitorização de sessões remotas e da imposição de métodos de autenticação multi-fator em todas as atividades realizadas;

- Explorar a utilização de ferramentas e metodologias de classificação de ativos de informação, como o *Azure Information Protection*[13] para ambientes *Windows*. A implementação de uma destas ferramentas aumentaria consideravelmente o nível de maturidade do repositório de ativos da organização, através de funcionalidades como a classificação, *marking* e controlo de acessos a documentos e *e-mails*.

Bibliografia

[1] M. Chapple, J. M. Stewart e D. Gibson. *(ISC)² CISSP certified information systems security professional: official study guide*. John Wiley Sons, 2018.

[2] E. Coyne e T. R. Weil. "ABAC and RBAC: scalable, flexible, and auditable access management". Em: *IT Professional* 15.3 (2013), pp. 14–16.

[3] R. Dias. *The 5 Factors of Authentication*. https://medium.com/@renansdias/the-5-factors-of-authentication-bcb79d354c13. Dez. de 2017.

[4] EY. *Cybersecurity Academy*. 2019. URL: https://sites.ey.com/sites/MLDH/SitePages/CybersecurityAcademy.aspx (acedido em 15/03/2019).

[5] Gartner. *Magic Quadrant for Identity Governance and Administration*. 2018. URL: https://b2bsalescafe.files.wordpress.com/2018/03/magic-quadrant-for-identity-governance-and-administration.pdf/ (acedido em 15/09/2019).

[6] Gartner. *Magic Quadrant for Privileged Access Management*. 2018. URL: https://lp.cyberark.com/gartner-mq-pam-leader/ (acedido em 15/09/2019).

[7] Gartner. *Magic Quadrant for Access Management*. 2019. URL: https://www.okta.com/resources/access-management-leader-gartner-magic-quadrant/ (acedido em 15/09/2019).

[8] A. Gordon. *Official (ISC)2 Guide to the CISSP CBK, Fourth Edition*. Taylor e Francis, 2015.

[9] U. G. O. of Government Commerce. *Information Technology Infrastructure Library (ITIL)*. 2019. URL: https://www.itlibrary.org/ (acedido em 15/03/2019).

[10] ISACA. *COBIT*. 2019. URL: http://www.isaca.org/cobit/pages/default.aspx (acedido em 15/03/2019).

[11] KPMG. "European Identity and Access Management Survey". Em: (2009).

[12] Microsoft. *Active Directory Domain Services Overview*. 2017. URL: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview (acedido em 15/03/2019).

[13] Microsoft. *What is Azure Information Protection?* 2019. URL: https://docs.microsoft.com/en-us/azure/information-protection/what-is-information-protection/ (acedido em 15/09/2019).

[14] S. Osborn, R. Sandhu e Q. Munawer. "Configuring role-based access control to enforce mandatory and discretionary access control policies". Em: *ACM Transactions on Information and System Security* 3.2 (2000), 85–106. DOI: 10.1145/354876.354878.

[15] B. Rogers e M. Gale. *Why 84% Of Companies Fail At Digital Transformation*. 2016. URL: https://www.forbes.com/sites/brucerogers/2016/01/07/why-84-of-companies-fail-at-digital-transformation/#18184ce2397b (acedido em 15/03/2019).

[16] R. S. Sandhu. "Role-based access control". Em: *Advances in computers*. Vol. 46. Elsevier, 1998, pp. 237–286.

[17] R. S. Sandhu e P. Samarati. "Access control: principle and practice". Em: *IEEE communications magazine* 32.9 (1994), pp. 40–48.

[18] S. K. (SoftwareSecured). *Comparing the top 3 federated identity providers - OpenID, SAML, OAuth*. Nov. de 2018. URL: https://www.softwaresecured.com/federated-identities-openid-vs-saml-vs-oauth/ (acedido em 15/03/2019).

[19] I. O. for Standardization. *ISO/IEC 27002:2013*. 2013. URL: https://www.iso.org/standard/54533.html (acedido em 15/03/2019).

[20] J. G. Steiner, B. C. Neuman e J. I. Schiller. "Kerberos: An Authentication Service for Open Network Systems." Em: *Usenix Winter*. Citeseer. 1988, pp. 191–202.

[21] "The Oauth 2.0 Authorization Framework". Em: (2012). DOI: 10.17487/rfc6749.

[22] E. Young. "Identity and Access Management, Beyond Compliance". Em: (mai. de 2013).